

SEPTEMBER 2026

10DLG

COMPLIANCE HANDBOOK 2026

10dlc
COUNCIL

Quickstart Guide

[Section 1 Introduction](#)

This section outlines the purpose and objectives of this handbook. It provides an overview of the 10DLC ecosystem, crucial roles and responsibilities within the ecosystem, and key components that underpin its operation. This section also introduces the pivotal role of The Campaign Registry (TCR) and emphasizes the fundamental importance of 10DLC compliance to ensure campaign approval, message deliverability, and avoid messaging disruptions and penalties.

[Section 2 Brand and Campaign Registration](#)

This section provides a comprehensive guide to the 10DLC registration process. It details the steps and requirements for compliant brand and campaign registration, including identity verification and brand vetting. It also provides guidance on the selection of the appropriate campaign use case and the process of number association after registration is completed.

[Section 3 Campaign Review and Approval](#)

This section outlines the stages of campaign review. It provides insights into why campaigns might be rejected and offers resolution strategies for addressing these issues. It also provides an overview of campaign approval timelines and the use of compliance checklists to streamline the registration process.

[Section 4 Best Practices for Compliant Messaging](#)

This section covers guidelines for responsible and effective messaging via 10DLC. It covers the importance of consumer consent and provides information on compliant terms and conditions and privacy policies. It outlines content restrictions, rules for specific use cases, and other messaging best practices.

[Section 5 Appendix](#)

This section serves as a valuable resource hub, providing example messages and call-to-actions to illustrate compliant message programs. It also compiles a list of additional resources offering further avenues for information and support.

Version History				
Version	Date	Notes	Contributor(s)	Company
1.0	September, 2026	Initial version	Meredith Wiegman	Vonage
			TJ Thinakaran	CasselRoad
			David Schwind	Sinch
			Sarah Giraldi	EZ Texting
			Noelle Meyers	Infobip
			Danielle Nowicki	Infobip
			Denise Casey	Cisco
			Jacqueline Sarkies	Bandwidth
			Luke Thompson	Bandwidth
			Trevor MacDonald	Syniverse

Contents

1. Introduction	1
1.1 About this Handbook	1
1.2 Understanding the 10DLC Ecosystem	1
1.2.1 Overview	1
1.2.2 Roles and Responsibilities	1
1.2.3 Key Components	2
1.2.4 The Campaign Registry (TCR)	3
1.3 Understanding 10DLC Compliance	3
1.3.1 Overview	3
1.3.2 Notice of Noncompliance	3
1.3.3 Suspension	4
1.3.4 Consumer vs. Non-Consumer Messaging	4
2. Brand and Campaign Registration	4
2.1 Overview	4
2.2 Brand Registration, Verification, and Vetting	5
2.2.1 Compliant Brand Registration Requirements	5
2.2.2 Brand Identity Verification	7
2.2.3 Authentication+	7
2.2.4 Brand Vetting	8
2.2.5 Brand Appeals	8
2.3 Campaign Registration and Use Cases	9
2.3.1 Compliant Campaign Registration Requirements	9
2.3.2 Use Case Selection	12
2.3.3 Standard Use Cases	13
2.3.4 Special Use Cases	15
2.4 Number Association	17
2.4.1 Number Pooling	17
3. Campaign Review and Approval	17
3.1 Overview	17
3.2 Campaign Service Provider (CSP) Responsibilities for Campaign Review	18
3.3 Types of Review	18
3.3.1 Mobile Network Operator (MNO) Campaign Review	18
3.3.2 Brand Review	18
3.3.3 Campaign Review	18
3.4 Campaign Rejection Categories	19
3.5 Resolution Strategies	20
3.6 Campaign Approval Timelines	20
3.7 Compliance Checklists	21
4. Best Practices for Compliant Messaging	21
4.1 Overview	21

4.2 Consumer Consent	21
4.3 Opt-in Requirements	22
4.3.1 Opt-in Method	22
4.3.2 Double Opt-in	22
4.3.3 Call-to-Action	22
4.3.4 Opt-in Confirmation Message	23
4.3.5 Opt-in Requirements for Single and Recurring Message Programs	23
4.4 Opt-out Requirements	23
4.5 Policy Requirements	24
4.5.1 Terms and Conditions	24
4.5.2 Privacy Policy	24
4.5.3 Privacy Principles	25
4.6 Disallowed and Restricted Content	26
4.6.1 Disallowed Content	26
4.6.2 Restricted Content	26
4.7 Restricted Use Cases	27
4.7.1 Sweepstakes and Contests	27
4.7.2 Political Campaigns	27
4.7.3 Charitable Donations	27
4.7.4 Sole Proprietors	28
4.7.5 Unified Communications as a Service (UCaaS)	28
4.7.6 Platform Free Trial (PFT)	28
4.8 Compliant Messaging Practices	29
4.8.1 Campaign Drift	29
4.8.2 Embedded Links and Phone Numbers	29
4.8.3 Message Frequency and Timing	29
4.8.4 Message Throughput	29
4.8.5 Snowshoe Messaging	30
4.8.6 Message Content Monitoring	30
4.8.7 Messaging Security	30
5. Appendix	30
5.1 Example Messages and Call-to-Actions	30
5.1.2 Example Message Templates	31
5.1.3 Example Call-to-Actions	32
5.2 Additional Resources	34
5.2.1 Messaging and Compliance Resources	34
5.2.2 Regulatory Resources	34
5.2.3 Industry Organizations	34
5.2.3 The Campaign Registry (TCR) Resources	34

1. Introduction

1.1 About this Handbook

10DLC (10-Digit Long Code) is a carrier-sanctioned system for non-consumer (application-to-person or A2P) messaging that uses local 10-digit phone numbers in the North American Numbering Plan (NANP). The purpose of this handbook is to provide guidance for the launch and operation of 10DLC message programs in the United States, with an emphasis on preserving the integrity of the 10DLC messaging ecosystem and ensuring consumer trust.

This handbook is a product of the 10DLC Council, a group of leading industry organizations providing expertise on 10DLC messaging. The content has the broad agreement and backing of mobile network operators (MNOs), ensuring alignment with their policies for a compliant and reliable 10DLC messaging ecosystem.

This handbook does not provide legal advice and should not be used in place of legal counsel. Message senders are responsible for adhering to all applicable laws and regulations, industry guidelines including [CTIA Messaging Principles and Best Practices](#), as well as individual MNO policies and terms of use¹.

Organizations within the 10DLC ecosystem may have specific requirements, processes, and policies that supplement the guidelines in this handbook. Message senders are strongly encouraged to work closely with their connectivity partners to understand partner-specific requirements.

1.2 Understanding the 10DLC Ecosystem

1.2.1 Overview

10DLC offers a carrier-sanctioned channel for non-consumer messages that provides transparency into who is sending messages and for what purpose. It enables reliable messaging using local 10-digit phone numbers with throughput levels suitable for business message programs. 10DLC aims to provide efficient, compliant, and spam-free communication that enhances customer engagement and trust.

10DLC messaging relies on a connectivity chain, where a sequence of connected partners facilitates the transmission of messages from the originating company to the intended recipient. 10DLC message program information is shared along this connectivity chain to ensure transparency and compliance.

1.2.2 Roles and Responsibilities

Roles and responsibilities in the 10DLC ecosystem include:

¹ See [Section 5.2 Additional Resources](#)

Role	Responsibilities
Consumer	An individual person who subscribes to wireless messaging services or apps and receives messages from brands. Also referred to as a user, customer, or subscriber.
Brand	The company, business, organization, or entity sending the message as perceived by the consumer.
Reseller	A company, such as an independent software vendor (ISV) or service provider, that acts as an intermediary between a CSP and a brand and has a direct relationship with the brand.
Campaign Service Provider (CSP)	A company that provides a 10DLC messaging platform or service and works with multiple brands and/or resellers to register 10DLC message program information in TCR.
Connectivity Partner (CNP)	A company that enables connectivity into carrier networks by providing a connection between CSPs and DCAs.
Direct Connect Aggregator (DCA)	A company that provides a direct connection to the mobile carrier networks to enable message delivery. A DCA may interconnect with other DCAs to broaden their network reach.
The Campaign Registry (TCR)	A centralized database and system chosen by MNOs to collect brand and campaign data for transparency on the 10DLC channel.
Verification/Vetting Provider	A company that assesses the identity of a brand before it can send messages and/or offers vetting services to determine eligibility for access to higher messaging throughput or special use cases.
Mobile Network Operator (MNO)	A company that provides the network, infrastructure, and messaging service to the subscriber. Also referred to as carrier, mobile carrier, operator or wireless provider.
netnumber Services Registry (nnSR)	An authoritative message routing registry used to manage and distribute routing and A2P campaign information for 10DLC messaging.

1.2.3 Key Components

Key components of the 10DLC ecosystem include:

Component	Description
Message	An SMS (text) or MMS (multimedia) message sent to or from a phone number.
Campaign	The message program that will be sent by the brand for a specific use case and includes details such as content and opt-in procedures.
Use Case	The purpose and nature of the messages a brand intends to send via a 10DLC campaign.

Registration	The process of submitting required information about the sending entity (brand) and the message program (campaign) to TCR.
Connectivity Chain	A sequence of connected partners, such as a CSP, CNP, and DCA, that facilitate the transmission of messages from the originating company to the intended recipient. Participants in the connectivity chain may be referred to as partners, delivery partners, or connectivity partners.

1.2.4 The Campaign Registry (TCR)

TCR plays a role as the centralized hub for the 10DLC ecosystem. It is designated by the MNOs to collect brand and campaign information, providing transparency into who is sending messages and for what purpose. It facilitates 10DLC registration and brand identity verification and provides the infrastructure that allows the 10DLC messaging ecosystem to operate with greater accountability and transparency. **However, TCR is not a compliance organization and does not offer guidance on compliance-related issues or enforce compliance requirements.** TCR does not review, approve or reject 10DLC campaigns, nor enforce or lift traffic suspensions.

1.3 Understanding 10DLC Compliance

1.3.1 Overview

All 10DLC message programs and content must comply with the [CTIA Messaging Principles and Best Practices](#), individual MNO policies and terms of use, and all applicable federal and state laws and regulations.²

Prior to the launch of a 10DLC message program, partners in the connectivity chain will review the campaign for compliance with applicable guidelines, policies or regulations. If a connectivity partner determines that a campaign is not compliant, the campaign may be rejected.³

Post approval and launch of a 10DLC message program, partners in the connectivity chain will at their discretion conduct routine monitoring, reviews, or audits of campaigns and message content to ensure compliance with applicable guidelines, policies or regulations. Noncompliance may lead to message blocking, suspension of messaging services and/or fines, in accordance with individual connectivity partner or MNO policies.

1.3.2 Notice of Noncompliance

If a 10DLC message program is found to be noncompliant after launch, partners in the connectivity chain may provide written notice of noncompliance to the responsible party.

Audits or notices of noncompliance will aim to clearly identify the following (as applicable):

² See [Section 5.2 Additional Resources](#)

³ See [Section 3 Campaign Review and Approval Process](#)

- Nature of the violation
- Description of severity
- Request for a written response
- Time frame for written response
- Outline any information that is required in the response. For example, root cause and corrective actions.

1.3.3 Suspension

Suspension signifies a temporary or permanent cessation of 10DLC messaging services imposed by partners in the connectivity chain, such as a DCA or MNO. Suspension may be prompted by noncompliance with industry guidelines, or violations of policies or regulations.

Suspensions may occur at a campaign level or may impact all campaigns associated with a brand. Addressing a suspension typically requires the brand to take specific steps in collaboration with the entity that initiated the suspension. However, it's important to note that reinstating a suspended 10DLC message program is not guaranteed.

1.3.4 Consumer vs. Non-Consumer Messaging

The 10DLC ecosystem observes the differentiation between Consumer and Non-Consumer messaging as defined in the [CTIA Messaging Principles and Best Practices](#).

As all business messaging via local 10-digit phone numbers is considered non-consumer, it requires registration under the 10DLC framework. Brands should consult with their CSP to understand partner-specific and/or MNO requirements regarding classification of Consumer vs. Non-Consumer messaging.

2. Brand and Campaign Registration

2.1 Overview

10DLC registration is a process in which a brand partners with a CSP to register their company information (brand) and message program (campaign) with TCR. The CSP then works with a CNP or DCA to associate the campaign with a phone number to enable compliant business messaging. 10DLC registration incurs one-time or recurring fees for brand registration, brand vetting, brand appeals, and campaign registration, as applicable. Brands should consult with their connectivity partner for guidance on the applicable fees associated with their 10DLC registration.

It is important to note that each partner in the connectivity chain may have different requirements for 10DLC registration. Brands should work closely with their connectivity partner to understand these differences, including referring to partner-specific documentation, such as FAQs, checklists or guidelines.

2.2 Brand Registration, Verification, and Vetting

The first step in the 10DLC registration process is brand registration. Brand registration provides information about the business associated with the message program. Brands intending to communicate with consumers via the 10DLC messaging channel must work with a CSP or reseller partner to complete brand registration with TCR. Upon brand registration, TCR assigns a brand ID. The brand ID is a unique, 7-character, alphanumeric identifier, starting with the letter “B”. A single brand may have multiple brand IDs if the brand registers multiple times using the same Tax ID/Employer Identification Number (EIN).

2.2.1 Compliant Brand Registration Requirements

The following table details compliance requirements for brand registration. This table does not represent all mandatory brand registration fields but rather focuses on the specific compliance requirements of brand properties when they are provided.

Furthermore, **all brand information must accurately represent the business that the end user believes is sending the message**, not a third party such as an ISV, reseller, or parent company.

Brand Property	Description	Compliance Requirements
Brand Entity	The legal classification of the business or organization sending messages. Entity types include: • Private • Publicly traded • Non-profit • Government • Sole proprietor	• Accurately reflects the entity type of the business
Employer Identification Number (EIN) ⁴ / Tax ID	A unique identifier that is the brand's registration number with the tax authority of their governing country.	• Matches the tax ID registered with the tax authority of the brand's governing country • Represents the tax ID of the brand identified in the message content, not a parent company or other party
Legal Company Name	The official name of the business registered with the tax authority of the brand's governing country.	• Matches the name registered with the tax authority of the brand's governing country • Represents the legal name of the brand identified in the message content, not a parent company or other party

⁴ EIN is specific to US businesses and is a nine-digit number in the format XX-XXXXXXX.

Brand Property	Description	Compliance Requirements
Doing Business As (DBA) Name	The name under which the business or organization operates publicly.	• Demonstrates an easily identifiable relationship with the legal name⁵ • Represents the DBA name of the brand identified in the message content, not a parent company or other party
Brand Physical Address	The actual, geographical location of the business or organization.	• Matches the address registered with the tax authority of the brand's governing country • Accurate and up to date
Brand Website	The online presence of the brand.	• Demonstrates a clear relationship with the registered brand name or DBA name⁶
Brand Relationship	The relationship level that reflects the history and trust a CSP has with a specific brand. Relationship categories include: • Basic accounts • Small accounts • Medium accounts • Large accounts • Key accounts	• Accurately reflects the relationship standing of the brand with the CSP
Brand Vertical	The category that describes the type of business or business operations of a brand. Examples include: • Real Estate • Healthcare and Life Sciences • Retail and Consumer Products • Financial Services • Information Technology Services	• Accurately reflects the brand's operations or type of business
Brand Support Contact Information	The email address and phone number that allows MNOs, CSPs, or DCAs to contact the brand if any issues arise during or after the registration process. ⁷	• Operational/working state • Branded email address (e.g., support@brand.com)⁸

⁵ If the relationship between the legal and DBA names is not evident, the brand should provide a clear explanation of the relationship in the campaign description, and/or supporting documentation that demonstrates the relationship.

⁶ Partner-specific requirements may vary. In some cases, such as small businesses or sole proprietors, a social media page or online directory link may be accepted, or a website may be omitted.

⁷ May be different from the brand's contact information that is used for customer support in the HELP message response.

⁸ Partner-specific requirements may vary. In some cases, such as small businesses or sole proprietors, personal/free email domains may be accepted.

Brand Property	Description	Compliance Requirements
Brand Business Contact Email	Employee email address associated with a publicly traded business in order to complete an additional identity verification process called Authentication+. ⁹	• Not a personal/free email domain • Not a common email distribution address (e.g., support@brand.com) • Validated via 2FA

2.2.2 Brand Identity Verification

When a brand is registered with TCR, a verification provider verifies the identity of the brand and TCR issues a brand identity status based on the verification provider's assessment. Brands must have either a verified or vetted verified status before campaign registration can occur. Brand verification may also validate additional brand attributes when applicable, such as non-profit or government entity status, or inclusion on the Russell 3000 stock market index.

Brand identity statuses include the following:

- **Verified:** Indicates a brand whose EIN, legal company name and legal company address could be confirmed by the verification provider.¹⁰
- **Vetted Verified:** Indicates that the brand has completed additional vetting.
- **Unverified:** Indicates that the identity of the brand could not be confirmed by the verification provider due to issues such as inaccurate or outdated information.¹¹

2.2.3 Authentication+

Publicly traded brands must complete an additional identity verification process, called Authentication+, to prevent brand impersonation and consumer fraud by requiring brand personnel attestation. As part of this process, the brand provides a business contact email address during brand registration which is validated via a verification PIN. Authentication+ verification must be completed before a publicly traded brand can register a campaign.¹²

2.2.4 Brand Vetting

Brands may choose to apply for vetting to unlock higher messaging throughput or to access special use cases for some MNO networks. Vetting is performed by a vetting provider who verifies the brand's legitimacy and typically produces a vetting score that can improve brand/campaign throughput level with some carriers. A vetted brand obtains a vetted verified identity status upon completion of vetting. Depending on the type of vet requested, the availability of the vetting result may vary from a few minutes to a few weeks. If a brand receives a vetting score that is excessively low, it may be subject to additional scrutiny from some partners in the connectivity chain prior to campaign approval.

⁹ See [Section 2.2.3 Authentication+](#)

¹⁰ For sole proprietor brands, a verified status is obtained via brand data validation and OTP validation, not a verification provider. See [4.7.4 Sole Proprietors](#).

¹¹ Unverified brands cannot register campaigns. To resolve an unverified status, the brand may need to correct and resubmit brand details or submit a brand identity appeal. See [Section 2.2.5 Brand Appeals](#)

¹² See [TCR Authentication+ Documentation](#)

Vetting types include the following:

- **Standard Vet:** An automated review performed by a vetting provider of a brand's history, employee count, and other factors. A standard vet returns a score from 0-100.
- **Enhanced Vet:** A manual review performed by a vetting provider of a brand's history, lawsuits, employee count, and other factors. It is typically requested after a standard vet and may or may not result in an increased vetting score. An enhanced vet returns a detailed report as well as a score from 0-100.
- **Political Vet:** Verification performed by a vetting provider confirming that the political entity is properly registered for participation in U.S. elections and is required by some MNOs to send political messaging. A political vet results in a token or status that allows access to the political campaign use case.¹³

2.2.5 Brand Appeals

An appeal allows a brand to dispute an unverified identity status or dispute a standard vet that failed or has a low score by submitting additional supporting documentation via TCR to the vetting provider, subject to certain requirements and deadlines.

Reasons for identity status appeals include the following:

- Verifying an unverified brand if the information provided is believed to be accurate
- Verifying the identity status of international brands outside the US
- Verifying the tax ID for public, private and non-profit organizations and government entities
- Verifying non-profit status/subsection for non-profit organizations
- Verifying government status for government entities

Reasons for vetting appeals include the following:

- Appealing a failed standard vet
- Appealing a low vetting score if the vetting score is believed to be too low based on the brand's characteristics

2.3 Campaign Registration and Use Cases

After brand registration, the next step in the 10DLC registration process is campaign registration. Campaign registration provides details about the use case, content, and attributes of the brand's message program. Campaign registration can only occur after the brand has obtained a verified or vetted verified status. Upon campaign registration, TCR assigns a campaign ID. The campaign ID is a unique, 7-character, alphanumeric identifier, starting with the letter "C". A brand may register multiple campaigns as applicable to support various messaging use cases.

¹³ See [4.7.2 Political Campaigns](#)

2.3.1 Compliant Campaign Registration Requirements

The following table details compliance requirements for campaign registration. This table does not represent all mandatory campaign registration fields, but rather focuses on the specific compliance requirements of campaign properties when they are provided.

Campaign Property	Description	Compliance Requirements
Use Case	The purpose or type of content that is sent in the message program. ¹⁴	• Accurately reflects the production message content. If content reflects multiple use cases, all sub use cases should be selected. • Aligns with the campaign description and the sample message content.
Campaign Description	Explanation of the campaign's purpose.	• Clear and detailed description of what the campaign will be used for and how it aligns with the type of business/operations of the brand. • Aligns with the use case(s) and the sample message content.
Call-to-Action/Message Flow ¹⁵	Explanation of how users opt-in to receive messages (opt-in method). ¹⁶	• Clear and detailed description of all ways in which users opt-in, such as: ◦ Via a website form ◦ Texting an opt-in keyword ◦ At a point-of-sale (POS) display ◦ Via a hardcopy form ◦ Verbally in-person or via IVR
Call-to-Action/Message Flow	The specific invitation to the user to opt-in to a messaging campaign (call-to-action). ¹⁷	• Program/brand name that is consistent with the registered brand. • Message frequency disclosure (e.g., #msgs/mo, msg frequency varies).¹⁸ • Opt-out instructions (e.g., Reply STOP to cancel).¹⁸ • "Message and data rates may apply" disclosure. • Link to terms and conditions or complete terms and conditions. • Link to privacy policy or privacy policy declaration. • Age gate for age-restricted message programs.¹⁹

¹⁴ See [Section 2.3.2 Use Case Selection](#)

¹⁵ Call-to-action/message flow is a single field within the campaign registration record in TCR that is used to capture multiple elements related to opt-in method and call-to-action.

¹⁶ See [Section 4.3.1 Opt-in Method](#)

¹⁷ See [Section 4.3.3 Call-to-Action](#)

¹⁸ Not required for single message programs.

¹⁹ See [Section 4.6.2 Restricted Content](#)

Campaign Property	Description	Compliance Requirements
Terms and Conditions	The terms and conditions related to the message program. ²⁰	• Program/brand name that is consistent with the registered brand. • Opt-out instructions (e.g., Reply STOP to cancel). • Customer support contact information (e.g., Reply HELP for help). • Link to privacy policy or privacy policy declaration.
Privacy Policy	The policy that explains how user information is collected, used, and shared. ²¹	• Program/brand name that is consistent with the registered brand. • Confirmation that the mobile information of the end user opting in to the message program will never be shared with or sold to third parties or lead generators.
Supporting Documentation	Proof of call-to-action, terms and conditions, or privacy policy documents. ²²	• Evidence of all call-to-actions used (as applicable). Examples include: ◦ Screenshot of app-based opt-in ◦ Media upload of keyword advertisement ◦ Digital version of hardcopy form ◦ Verbal/IVR call-to-action script • Terms and conditions or privacy policy documentation (as applicable). • Text and visual elements that are legible and discernable.
Opt-in Message	The initial message confirming a user's subscription to a message program. ²³	• Program/brand name that is consistent with the registered brand.²⁴ • Opt-out instructions (e.g., Reply STOP to cancel). • Customer care contact information (e.g., Reply HELP for help). • Message frequency disclosure (e.g., #msgs/mo, msg frequency varies). • "Message and data rates may apply" disclosure.

²⁰ See [Section 4.5.1 Terms and Conditions](#)

²¹ See [Section 4.5.2 Privacy Policy](#)

²² The brand may upload or provide supporting documentation if the call-to-action, terms and conditions, or privacy policy are not available online or are otherwise not accessible.

²³ See [Section 4.3.4 Opt-in Confirmation Message](#)

²⁴ For single message programs, only the program/brand name is required to be included in the opt-in message.

Campaign Property	Description	Compliance Requirements
Opt-out Message	The message that is sent in reply to end users when they send an opt-out request (e.g., STOP keyword). ²⁵	• Program/brand name that is consistent with the registered brand. • Confirms that the user has unsubscribed and that no further messages will be sent.
HELP Message	The message that is sent in reply to end users when they send a help request (e.g., HELP keyword).	• Program/brand name that is consistent with the registered brand. • Includes customer care contact information (e.g., phone number, email address and/or URL that leads directly to a support contact webpage).
Sample Messages	Examples of the types of messages that will be sent from the campaign.	• Program/brand name that is consistent with the registered brand. • Aligns with the campaign use case and the campaign description. • Accurately represents the production message content. For campaigns with multiple use cases, all sub use cases should be represented. • Does not contain public URL shorteners.
Campaign and Content Attributes	Yes/No declarations indicating whether the campaign will use certain features or involve particular types of content.	• Accurate representation of applicable campaign and content attributes including: ◦ Message content containing embedded links or phone numbers.²⁶ ◦ Use case requiring number pooling.²⁷ ◦ Use case involving age-gated content.²⁸ ◦ Use case involving direct lending content.²⁸ • Affirmation that the campaign will not involve affiliate marketing²⁹
Reseller	Name of the ISV or service provider that sits between a CSP and the brand being registered.	• Accurately identifies the reseller, if registering a campaign on behalf of a reseller, or indicates if no reseller is involved.

2.3.2 Use Case Selection

A campaign use case defines the purpose and nature of the messages a brand intends to send. The use case selected during campaign registration can impact several aspects of a 10DLC message program, including:

²⁵ Not required for single message programs.

²⁶ See [Section 4.8.2 Embedded Links and Phone Numbers](#)

²⁷ See [Section 2.4.1 Number Pooling](#)

²⁸ See [Section 4.6.2 Restricted Content](#)

²⁹ See [Section 4.6.1 Disallowed Content](#)

- **Registration fees:** The cost of monthly campaign registration fees can vary depending on the use case selected.
- **Compliance requirements:** Some use cases may require additional vetting, approvals, or restrictions on use.
- **Message throughput:** Some MNOs allocate throughput rates or daily volume allowance based on use case.³⁰

Key considerations for use case selection include:

- The **core function and nature of the message program** rather than the vertical or intended audience. For example, a retail business might select the "Delivery Notifications" use case for order confirmations or the "Marketing" use case for promotional offers.
- **Volume requirements** that may influence use case selection. For example, brands that require low messaging throughput for varied purposes might select the "Low Volume Mixed" use case but might select other use cases for higher volumes or specific needs.
- Where applicable, **dedicated/single use case campaigns are strongly preferred** to ensure alignment and clarity between the declared use case, campaign description, and sample messages.

Brands should consult with their connectivity partner for guidance to make the most appropriate use case selection. CSPs may also consult with their partners in the connectivity chain to obtain DCA or MNO guidance or approval for appropriate use case selection, as applicable. If none of the available use case options fit the purpose of the message program, brands should select the use case that most closely aligns with the nature of their message program and provide additional clarifying details on the purpose of the use case in the campaign description.

Selecting the incorrect use case may lead to campaign rejection or insufficient message throughput. In addition, it is important to select the appropriate use case to prevent campaign drift³¹. Campaign use case cannot be changed after registration. In case of inappropriate use case selection, the brand will need to register a new campaign with the appropriate use case.

2.3.3 Standard Use Cases

The following tables detail standard use cases that are readily available for registered and verified brands and do not require approval by MNOs. While vetting is not required to register standard use cases, partner-specific vetting requirements to access standard use cases may vary.

Informational message programs <i>Not intended for promotional content</i>		
Use Case	Description	Examples
2FA (Two-Factor Authentication)	Sending security codes or one-time passwords (OTPs) to verify user identities or to verify security-related information.	• OTP to confirm account login • Security code to verify profile update

³⁰ See [Section 4.8.4 Message Throughput](#)

³¹ See [Section 4.8.1 Campaign Drift](#)

Account Notifications	Important and relevant updates or alerts to customers or users about their accounts, typically triggered by specific events or changes related to the account.	• Account transaction alerts • Account balance reminders • Profile update alerts
Customer Care	Direct support and assistance to customers through two-way messaging conversations that enables customers to ask questions, seek help, resolve issues, and manage their accounts.	• Responding to customer inquiries • Troubleshooting customer issues
Delivery Notifications	Real-time updates and alerts to customers regarding the status of their orders or deliveries or related to the logistics and progress of order fulfillment.	• Shipment updates • Delivery confirmations
Fraud Alert Messaging	Urgent notifications to customers regarding potential or suspected fraudulent activity detected on their accounts.	• Alerts for unauthorized charges • Compromised payments alerts
Higher Education	Messages from colleges, universities or other educational institutions to facilitate communication with students, faculty, staff or alumni. This use case is not for free messaging models.	• Class scheduling updates • Campus event notifications • Enrollment updates
Polling & Voting	Non-political surveys, polls, and voting initiatives appropriate for gathering feedback, conducting market research, or facilitating decision-making processes in non-political contexts. This use case is not for political message programs.	• Customer satisfaction surveys • Product feedback polls • Employee opinion surveys
Public Service Announcement	Messages that benefit the community or address matters of public interest.	• Community event reminders • Utility outage alerts • Road closure notifications
Security Alert	Alerts related to a security compromise of a hardware or software system that requires the user to take action.	• Software security alerts • Smart home security alerts

Promotional message programs		
Use Case	Description	Examples
Marketing	Any communication that includes marketing and/or promotional content sent to customers or potential customers designed to generate interest, drive sales, or promote products or services.	• Sending coupons • New sale announcements • Abandoned shopping cart notifications

Mixed message programs <i>Promotional and/or informational content</i>		
Use Case	Description	Examples
Low Volume Mixed	Brands with multiple use cases that anticipate sending very low message volumes. May include promotional content. A minimum of two and a maximum of five sub-use cases can be selected.	• Test/demo accounts • A small business sending promotional and customer care messages
Mixed	Brands with multiple use cases but with volume or content that does not fit the criteria for the Low Volume Mixed use case. May include promotional content. A minimum of two and a maximum of five sub-use cases can be selected.	• A retailer sending marketing messages, delivery notifications and customer care messages

Non-subscriber facing message programs		
Use Case	Description	Examples
Machine-To-Machine (M2M)	Messages where no human interaction is involved. Refers to processes that involve wireless communication between two or more physical assets. This use case is not for subscriber-facing message programs. Compliance requirements related to consent, required disclosures, or policy documentation typically do not apply to this use case.	• Remote monitoring • Data collection • Control of automated systems

2.3.4 Special Use Cases

The following tables detail special use cases that involve sensitive content which require closer scrutiny due to potential impact. These use cases may require brand vetting or pre/post-registration approval by MNOs to ensure compliance and prevent misuse. Requirements for special use cases can vary by MNO. CSPs intending to support special use cases that require CSP pre-approval by MNOs, or separate contractual terms, reporting, or controls, should consult with TCR for specific details and requirements.

Post-registration approval by MNO required		
Use Case	Description	Examples
Agents and Franchises	Brands that need to support messaging with multiple agents, franchises, or offices in the same vertical that need individual localized numbers. Limited to 5,000 numbers.	• Real estate agents communicating with buyers • Insurance brokers communicating with customers

Carrier Exemptions	Brands that have a pre-existing exemption granted by a specific carrier.	Exemptions for unique circumstances
Emergency	Notification services that support public safety and health during emergencies.	- Severe weather alerts - Public health alerts
K-12 Education	Schools from kindergarten through 12th grade and distance learning centers communicating with students, parents, and faculty. Message services must be provided to schools for free.	- Teachers sharing classroom updates with students and parents - Schools sharing event reminders
Proxy	Peer-to-peer and app-based group messaging while protecting users' privacy by using proxy or pooled numbers.	Proxy numbers for ride-sharing services
Sweepstakes	Messaging related to sweepstakes and contests characterized by the element of chance and the awarding of a prize.	- Radio station contest for concert tickets - Retail store drawing for a prize

Non-profit entity type or additional vetting required		
Use Case	Description	Examples
Charity	Registered charitable organizations classified as 501(c)3 entities communicating with donors and beneficiaries.	- Charity fundraising alerts - Charity event notifications
Political	Communication from political campaigns, political action committees, or organizations engaging in political activities. A political vet is required for non-profit brands without a 501(c)(3/4/5/6) tax-exempt status to access this use case.	- Communication from a candidate running for office - A political party promoting its platform

MNO pre-approved CSP required		
Use Case	Description	Examples
Public Safety (Restricted)	Brands that have a pre-existing exemption granted by a specific carrier. Restricted class of service not available to the public. Post-registration approval by MNOs is also required for this use case. Brands should consult with their connectivity partner to understand the appropriate use of this campaign type.	Brands operating in regulated industries that require special considerations

Social	Public figures, influencers, or celebrities who want to engage with their communities through messaging.	• A social media influencer sharing updates with fans • A musician promoting an upcoming tour
UCaaS High Volume	UCaaS companies with higher messaging volume requirements to facilitate diverse business communications.	• A large enterprise using UCaaS for internal and customer communication
UCaaS Low Volume	Unified Communications as a Service (UCaaS) companies with lower messaging volume needs to facilitate diverse business communications.	• A small business using UCaaS for internal and customer communication

Separate CSP contractual terms, reporting and messaging controls required		
Use Case	Description	Examples
Platform Free Trial	CSPs and ISVs that offer free trial services to their new 10DLC non-paying customers, allowing end users to test messaging services.	• A company offering a free trial of its 10DLC messaging platform
Sole Proprietor	Individuals or small businesses operating as sole proprietorships in the US or Canada without an EIN or Tax ID. Mixed content with a minimum of one and a maximum of five sub-use case selections allowed. Restricted to a single number per campaign.	• A local handyman communicating with customers • A small online retailer operating as a sole proprietorship sending order confirmations

2.4 Number Association

Number association is the process of linking a 10-digit local phone number to a 10DLC campaign. Upon campaign registration, TCR publishes the campaign ID in the nnSR. Subsequently, the CNP or DCA provisions the 10DLC phone number(s) in the nnSR with a netnumber ID (NNID), which identifies the messaging service provider, and flags the phone number(s) with the campaign ID and other A2P properties. Some MNOs also require that DCAs provision 10DLC phone numbers and brand/campaign information in their platforms prior to initiation of 10DLC messaging. The 10DLC number association process ensures accurate message routing, transparency, and traceability within the 10DLC ecosystem.

2.4.1 Number Pooling

Number pooling is a process by which a pool of numbers is associated with a single campaign. 10DLC primarily makes number pools unnecessary by allocating message throughput based on a brand's vetting status and use case, rather than the quantity of phone numbers associated with the campaign. However, a number pool may be used for certain use cases which require a large number of phone numbers, such as proxy services, agents and franchises, or UCaaS applications. Use cases requiring a number pool to send similar content may require partner or MNO approval and a

different provisioning process on some carrier networks. The brand must specify whether the campaign will use a number pool by selecting the corresponding campaign content attribute as part of the campaign registration record.

3. Campaign Review and Approval

3.1 Overview

The final step in the 10DLC registration process is campaign review and approval. After a brand partners with a CSP to complete registration of their brand and campaign with TCR, the CSP shares the campaign with their partner (a CNP or DCA) in the connectivity chain to handle message delivery. Upon receiving the campaign sharing request, the partner reviews the brand and campaign details for compliance with industry guidelines and carrier policies and has the option to accept or reject the campaign sharing request.

A campaign must be accepted by all partners in the connectivity chain before message program launch can occur. Some special use case campaigns require MNO approval prior to program launch. If a connectivity partner determines that a campaign is not compliant, they may reject the campaign sharing request and will share the reason for the rejection with the submitting entity. It is important to note that a campaign rejected by a partner does not indicate rejection by an MNO. MNOs have limited visibility into campaigns that are rejected by a connectivity partner.

3.2 Campaign Service Provider (CSP) Responsibilities for Campaign Review

CSPs are the initial point of contact for brands registering campaigns and hold a crucial responsibility in the early stages of the review process. CSPs must guide brands on providing accurate and comprehensive information required for compliant campaign registration, such as use case selection, campaign description, sample messages, opt-in methods, and campaign attributes. Furthermore, CSPs must guide brands on the critical importance of obtaining consumer consent, opt-out responsibilities, spam mitigation and other aspects of compliant 10DLC campaign operation.

3.3 Types of Review

3.3.1 Mobile Network Operator (MNO) Campaign Review

Some special campaign use cases may be subject to post-registration review by one or more MNOs. MNO review occurs prior to partner review. If an MNO rejects a campaign, they will share the reason for the rejection with the CSP. The brand should consult with their CSP partner to understand the resolution path for a campaign that has been rejected by an MNO. MNO campaign approval does not guarantee campaign approval by other partners in the connectivity chain.

3.3.2 Brand Review

As part of the campaign approval process, the partner in the connectivity chain will review brand details for compliance with industry guidelines and carrier policies, including the requirements as detailed in [Section 2.2.1 Compliant Brand Registration Requirements](#). Campaigns associated with brands that do not meet these requirements may be rejected.

3.3.3 Campaign Review

As part of the campaign approval process, the partner in the connectivity chain will review the campaign details for compliance with industry guidelines and carrier policies, including the requirements as detailed in [Section 2.3.1 Compliant Campaign Registration Requirements](#). Campaigns that do not meet these requirements may be rejected.

3.4 Campaign Rejection Categories

Campaign rejection categories are used by partners in the connectivity chain to classify the reasons why they have rejected a 10DLC campaign, in addition to providing a written explanation. The goal of these categories is to help brands identify and address potential compliance issues effectively.

Campaign rejection categories include:³²

Rejection Reason	Description	Common Examples	Reference Section(s)
Brand Inconsistencies	Brands must provide accurate details that match required fields for the brand type. Also, brand and campaign details must be consistent.	- Brand name on website does not match the registered or DBA brand name - Inaccurate contact information	Section 2.2.1 Compliant Brand Registration Requirements
Call-to-Action	The call-to-action must ensure consumers understand how to opt-in and consent to receive messages. It also must clearly display a program/brand name, message frequency, potential charges, a STOP keyword, and links to terms and conditions and privacy policies.	- Failure to describe the opt-in method - Call-to-action missing the message frequency disclosure	Section 2.3.1 Compliant Campaign Registration Requirements Section 4.3 Opt-in Requirements
Campaign Description/ Attributes	Campaign descriptions and attributes must align with the declared use case. A clear and concise description of the intended purpose of the campaign must be provided for the end user.	- Campaign description does not align with the declared use case - Failure to declare direct lending content	Section 2.3.1 Compliant Campaign Registration Requirements

³² See [TCR Mandatory Campaign Rejection Categories Documentation](#).

Rejection Reason	Description	Common Examples	Reference Section(s)
Disallowed Content	The campaign contains content related to gambling, drugs, hate speech, illegal activities, or high-risk services or content that is strictly prohibited.	• Vape shop promoting cannabis products • Cryptocurrency or stock trading alerts	Section 4.6 Disallowed and Restricted Content
Mandatory Message Terminology	Mandatory message terminology must include opt-in confirmation, opt-out confirmation, a help response, and required disclosures.	• Opt-in confirmation message missing opt-out instructions • Help response message does not contain support contact information	Section 2.3.1 Compliant Campaign Registration Requirements
Privacy Policy	A clear privacy policy must be provided to the consumer that explains how personal data is collected and used. No third-party sharing is allowed for marketing purposes. The privacy policy must also be consistent with brand information.	• Privacy policy fails to inform users about third party data sharing practices • Privacy policy does not clearly identify the registered brand	Section 4.5.2 Privacy Policy
Sample Message	Sample messages must align with the declared use case and cannot include disallowed content or public URL shorteners.	• Sample message missing the brand name • Sample message does not align with the declared use case	Section 2.3.1 Compliant Campaign Registration Requirements
Terms and Conditions	Clear terms and conditions must be provided that include information on message frequency, the campaign description, any fees, opt-in and opt-out instructions, customer care contact information, and a reference to the privacy policy. The terms and conditions must also be consistent with brand information.	• Terms and conditions missing support contact information • Terms and conditions do not clearly identify the registered brand	Section 4.5.1 Terms and Conditions
Other	This category can be used when a campaign is rejected for reasons that do not fit into the other categories.	• Incomplete entries • Patterns resembling snowshoe messaging	Section 4 Best Practices for Compliant Messaging

3.5 Resolution Strategies

If a campaign is rejected by a partner in the connectivity chain, the brand should consult with their CSP partner to revise the campaign before resubmitting for further campaign review. It's important to note that each partner in the connectivity chain may have different requirements or processes for resubmission of a rejected campaign. Brands should work closely with their CSP partner to understand these differences, including referring to partner-specific documentation, such as FAQs, checklists or guidelines, to remedy campaign rejections.

3.6 Campaign Approval Timelines

Campaign approval times can vary from a few days to several weeks depending on the complexity of the use case and the number of partners (CSPs, CNPs, DCAs) involved in the review process and connectivity chain. While review times can vary, providing complete and accurate information during brand and campaign registration can help expedite the review process. Brands should consult with their connectivity partner for specific timelines regarding campaign approval.

3.7 Compliance Checklists

To assist with compliance requirements, participants within the 10DLC ecosystem can incorporate checklists for pre-submission reviews, to reduce the risk of campaign rejections and ensure more efficient launch of their 10DLC message programs.

Checklists may cover aspects of campaign compliance, such as:

- Brand consistency
- Accurate and unique campaign description
- Clear call-to-action with opt-in/out instructions and required disclosures
- Accessible terms and conditions and privacy policy (that confirms mobile opt-in data will not be shared)
- Sample messages that align with the declared use case and contain the correct brand name
- Mandatory message terminology for opt-in, HELP and STOP messages
- Age gate (if applicable)
- No evidence of disallowed content or practices

4. Best Practices for Compliant Messaging

4.1 Overview

10DLC best practices are intended to ensure effective, compliant, and trusted messaging, helping organizations within the 10DLC ecosystem maintain a good sender reputation, avoid message blocking or penalties, and provide a positive experience for consumers. By following guidelines put forth in the CTIA best practices and MNO guidelines, organizations can leverage 10DLC messaging effectively while safeguarding consumer trust and maintaining compliance with industry standards.

4.2 Consumer Consent

Consent is the explicit agreement a consumer gives to receive messages from a specific brand for a specific purpose. Consent must be obtained before a business can send any messages from a 10DLC campaign to an end user.³³

Types of consent include:

- **Implied Consent:** The consumer initiates a text message exchange, and a business responds with relevant information, without the consumer providing prior verbal or written permission.
- **Express Consent:** The consumer gives a business their phone number and agrees to be contacted for a specific informational purpose, and this permission may be given via text message, on a form, on a website, or verbally.
- **Express Written Consent:** The consumer provides explicit written permission to receive promotional/marketing messages, such as by signing a form or checking a box online.

4.3 Opt-in Requirements

Opt-in is when a consumer gives prior consent to a brand to receive messages. Brands must document consent acquisition and maintain accurate consent records. Brands cannot transfer, assign, share or sell opt-in consent to affiliates or third parties.

4.3.1 Opt-in Method

The opt-in method is the mechanism or way in which the brand obtains consent from the consumer. A brand may use various opt-in methods to obtain consent, including the following:

- Via a website form
- Texting an opt-in keyword
- At a point-of-sale (POS) display
- Via a hardcopy form
- Verbally in-person, over the phone with an agent, or via interactive voice response (IVR) technology

4.3.2 Double Opt-in

Double opt-in is when the consumer provides consent via an initial opt-in and then responds affirmatively to a message from the brand to confirm their consent (e.g. Reply YES to confirm). Brands may use a double opt-in method if they obtained initial consent outside of the messaging channel, such as opt-in via a hardcopy form, at a point-of-sale (POS) display, or verbally. Double opt-in may also be used to ensure that the consumer genuinely intended to consent to the message program.

³³ See [CTIA Messaging Principles and Best Practices](#) for more information on types of messaging content and associated consent principles.

4.3.3 Call-to-Action

The call-to-action is the invitation from the brand, presented via the opt-in method(s), to the consumer to opt-in to the 10DLC campaign. It must be clear, conspicuous, and disclose the nature of the message program.

The call-to-action must include the following:

- Brand identity (brand or program name)
- Opt-in instructions
- Opt-out instructions (e.g., reply STOP to cancel)³⁴
- Messaging frequency³⁴
- “Message and data rates may apply” disclosure
- Terms and conditions and privacy policy, either in full or via clearly labeled links

Additional requirements for the call-to-action include the following:

- Regardless of consent type (implied, express, or express written consent), the brand must provide the necessary disclosures in the call-to-action.
- When a brand is collecting express written consent, the user must initiate consent. For example, if the brand uses an online checkbox to obtain express written consent, the checkbox cannot be selected by default.

4.3.4 Opt-in Confirmation Message

The opt-in confirmation message is the initial message sent by the brand to confirm the user's subscription to a recurring message program. A single opt-in confirmation message must be sent after a consumer opts into a campaign, except for message programs using a double opt-in approach, in which case multiple messages may be sent to confirm opt-in. For opt-ins obtained outside the messaging channel, such as at a point of sale (POS) or via a hardcopy form, the opt-in confirmation message must be delivered as soon as reasonably possible after the user opts in.

The opt-in confirmation message for a recurring message program must include the following:

- Brand identity (brand or program name)
- Opt-out instructions (e.g., reply STOP to cancel)
- Customer care contact information (e.g., Reply HELP for help)
- Messaging frequency
- “Message and data rates may apply” disclosure

4.3.5 Opt-in Requirements for Single and Recurring Message Programs

Single message programs are intended for a one-time exchange, delivering a single message in direct response to a consumer's opt-in action and consent, such as a two-factor authentication code. The call-to-action for a single message program must include all necessary disclosures except for the message frequency disclosure and opt-out instructions. The opt-in confirmation message (the

³⁴ Not required for single message programs.

message sent in response to the consumer's action) must contain the brand identity, but is not required to include any additional disclosures.

Recurring message programs involve an ongoing series of messages sent to a consumer after they provide consent, such as recurring marketing messages. Recurring message programs must include a message frequency disclosure and opt-out instructions in the call-to-action, along with all other necessary disclosures. The opt-in confirmation for a recurring message program must include the brand identity, messaging frequency, opt-out and help instructions, and the "message and data rates may apply" disclosure.

4.4 Opt-out Requirements

Opt-out is the process by which a consumer can revoke their consent to receive messages from a campaign and stop further communications. Recurring message programs must provide clear and accessible instructions for opting out (e.g., reply STOP to cancel). For recurring message programs, the campaign must include opt-out instructions at a minimum in the initial call-to-action, the opt-in confirmation message, and the terms and conditions. Brands should include opt-out instructions periodically within message content.

Brands must opt-out users that reply to the campaign with the keyword STOP. Along with the STOP keyword, the brand should honor reasonable equivalents as valid forms of opt-out, such as QUIT, END, CANCEL or UNSUBSCRIBE, or opt-outs using normal language such as "remove me from this list".

The brand must honor opt-out requests promptly and acknowledge the request with a single opt-out confirmation message. The brand must include in the opt-out confirmation message the brand or program name and an acknowledgement that the consumer is unsubscribed and will receive no further messages from the campaign. Opt-out requests apply to all phone numbers associated with the campaign, not just the individual number that received the opt-out request.

4.5 Policy Requirements

4.5.1 Terms and Conditions

Terms and conditions is the policy that outlines the brand's terms and conditions related to the message program. The brand must make messaging terms and conditions readily available and easily accessible to the end user, either through a clearly labeled link in the call-to-action, or by including them in full in the call-to-action.

The terms and conditions must outline the following:

- Brand name and message program details
- Information on how the consumer may opt-out (e.g., reply STOP to cancel)
- Customer support contact information (e.g., reply HELP for help)
- A privacy policy link or declaration

4.5.2 Privacy Policy

The privacy policy is the policy that outlines how the brand collects, uses, and shares consumer information. Brands must maintain a clear, accessible, easy to locate, and up-to-date privacy policy. Even if the brand's current privacy policy does not contain any language around data sharing, the privacy policy must confirm that the mobile information of the end user opting in to the message program will never be shared or sold to third parties or lead generators.

The privacy policy must explicitly state that mobile opt-in data (the end user's phone number) will not be shared or sold to third parties. Example statements include:³⁵

- "No mobile information will be shared with third parties/affiliates for marketing/promotional purposes"
- "Opt-in data and consent will not be shared with third parties."
- "All the above categories exclude mobile opt-in data, which will not be shared with third parties or affiliates."

The brand must make the privacy policy easily accessible, either through a clearly labeled link in the call-to-action, or a declaration in the call-to-action that mobile opt-in data will not be shared. In addition, a privacy policy link or declaration must be included in the terms and conditions. **However, it is important to note that partner-specific privacy policy requirements may vary.**

4.5.3 Privacy Principles

The following table outlines key principles for brands that can serve as a framework for privacy policy development and evaluation. **These principles are not intended as professional legal advice and should only be used as a starting point in consultation with legal counsel.**

Privacy Principle	Key Questions to Address	Privacy Objective
Data Collection and Use	• What consumer data is collected? • For what purposes is it used? • Is the purpose narrowly defined and necessary?	Ensure lawful, transparent data usage and limitation of its purpose.
Consent	• How is consumer consent obtained and is it appropriate for the type of messaging (e.g., informational vs promotional)? • Is opt-in initiated by the consumer? • Are consumers informed that they are agreeing to receive messages?	Establish valid consent in accordance with applicable regulations and industry guidelines.
Data Sharing and Selling	• Is it clearly stated that mobile data will not be shared or sold to third parties or affiliates? • Are service providers disclosed if used for message delivery?	Protect consumer data from unauthorized or undisclosed transfer.

³⁵ All examples are provided for informational purposes only and should not be used in place of legal counsel.

Privacy Principle	Key Questions to Address	Privacy Objective
Data Security and Storage	- How long is data retained and is that duration justified? - What safeguards are in place to protect stored data?	Prevent consumer data from data breaches and unauthorized access.
Opt-out Process	- Is the opt-out process clear and functional (e.g., reply STOP to stop)? - Is message delivery halted promptly upon opt-out?	Honor consumer requests to opt-out and comply with regulatory opt-out requirements
User Rights and Access	- Can users request access, correction, or deletion of their data? - Is there a mechanism in place to respond to user requests?	Provide consumer control and comply with access rights laws.
Regulatory Compliance	- Does the policy acknowledge compliance with relevant laws (e.g., TCPA, CCPA, GDPR)? - Have applicable regulations for mobile messaging, consumer data, and consent been reviewed with legal counsel?	Align with federal and state privacy regulations.
Accessibility	- Is the privacy policy easy to locate, clearly labeled, and written in a clear and understandable way? - Are there accommodations in accessibility or location of the policy for different business sizes (e.g., small businesses or sole proprietors)?	Promote privacy policy transparency, accessibility and usability for consumers.
Policy Updates	- Are changes to the policy communicated to users and what is the method of communication? - Is there a system in place to maintain version control?	Ensure up-to-date disclosures and consistency.

4.6 Disallowed and Restricted Content

4.6.1 Disallowed Content

Message content that is unlawful, harmful, misleading or violates carrier guidelines is not allowed on the 10DLC messaging channel. This includes the following categories³⁶:

- **Sexually Explicit and Hateful Content:** Content that is sexually explicit, hateful, violent, harassing, defamatory or obscene is not allowed.
- **Illegal Substances:** Content related to federally illegal drugs, such as cannabis, or controlled substances is not allowed.

³⁶ Content that is disallowed may include, but is not limited to, substances or activities that are federally illegal and/or not legal in all US states (e.g., cannabis, gambling). Some content may not be disallowed on all networks. Brands should consult their connectivity partner for guidance on content restrictions.

- **Affiliate Marketing and Lead Generation:** Content related to affiliate marketing, lead generation, or promotion of a third party's goods or services is not allowed. All promotional content must be directly related to the brand registered for the campaign. Brands must not use rented, sold, or shared opt-in lists and must obtain consent directly from consumers.
- **Fraud, Spam, and Deceptive Practices:** Content that is considered to be spam, fraudulent or misleading, or practices like phishing, smishing, social engineering and brand impersonation is not allowed.

4.6.2 Restricted Content

The following content categories are subject to specific restrictions or require additional compliance measures:

- **Age-Gated Content (Alcohol, Firearms, Tobacco):** Content related to age-restricted goods, such as alcohol, firearms or tobacco products, requires a robust age-gate mechanism to verify the consumer's age. The age-gate must be implemented at opt-in and require users to input their full date of birth to confirm they meet the minimum age requirement. A yes/no response or checkbox confirming minimum age is not considered an acceptable age gate. The brand must specify whether the campaign will support age-gated content by selecting the corresponding content attribute during the campaign registration process.
- **Financial Services:** Content related to high-risk financial services such as third-party lending, including short-term or payday loans, unsolicited debt collection, cryptocurrency, or other content that may lead to consumer financial harm, is not allowed. Content related to first party lending services or debt collection with express consent may be permitted. The brand must specify whether the campaign will support direct lending content by selecting the corresponding content attribute during the campaign registration process.
- **Job Boards:** Content involving generic alerts or promotions for jobs with entities other than the registered brand is generally not allowed, unless the consumer has specifically opted in to receive these messages from the third party.
- **Gambling:** Content related to gambling or betting is not allowed. However, brands associated with gambling, such as casinos or sports betting platforms, may be permitted to send content that is non-gambling in nature (e.g., 2FA codes, event notifications).

4.7 Restricted Use Cases

4.7.1 Sweepstakes and Contests

Sweepstakes and contest campaigns must adhere to applicable guidelines set forth by CTIA and MNOs³⁷. Official sweepstakes rules must be provided or easily accessible from the brand's website. Brands should consult with their connectivity partner to understand specific requirements related to sweepstakes campaigns. Sweepstakes campaigns require review and approval by some MNOs, which may add additional time to the campaign registration process.

³⁷ See [Section 5.2 Additional Resources](#)

4.7.2 Political Campaigns

Only non-profit brands that are 501(c)(3/4/5/6) or 527 tax-exempt organizations are eligible to register political use case campaigns. Some MNOs require 527 tax-exempt organizations to obtain a political vet to register a political use case campaign.³⁸ Political message programs must adhere to applicable guidelines set forth by CTIA and MNOs, including guidelines for obtaining acceptable consent.³⁹ Brands should consult with their connectivity partner to understand specific requirements related to political campaigns.

4.7.3 Charitable Donations

Charitable organizations soliciting donations via a 10DLC message program must select the Charity campaign use case during campaign registration. Charitable organizations must be classified as a 501(c)3 entity to access this use case⁴⁰ and should be accredited by a charity assessment organization.⁴¹ Charitable donation message programs must adhere to applicable guidelines set forth by CTIA and MNOs. Brands should consult with their connectivity partner to understand specific requirements related to charitable donation campaigns.

4.7.4 Sole Proprietors

Sole proprietors are small businesses and individuals in the US and Canada that do not have an EIN/Tax ID, typically reporting business income or losses on their individual income tax return. Only brands that do not have an EIN/Tax ID are qualified to register as sole proprietors. CSPs that wish to register sole proprietor message programs must have a separate contract with TCR to support this use case and submit a monthly report to TCR that covers their sole proprietor campaign activity. CSPs must cap sole proprietor daily message volume and throughput at carrier mandated limits. Brands should consult with their connectivity partner to understand specific requirements related to sole proprietor message programs.

Sole proprietor brands must complete a brand validation process prior to campaign registration. The validation process includes brand data validation, such as duplicate entry or well-formed data checks, as well as OTP verification via a mobile phone number. Sole proprietor brands are limited to a single campaign which can support mixed messaging content with up to five sub-use cases selections, and campaign number association is limited to a single phone number.⁴²

4.7.5 Unified Communications as a Service (UCaaS)

The UCaaS use case is designated for UCaaS companies providing cloud-based communication services to business customers where each number is typically associated with a different employee for diverse business communications. UCaaS use cases are not intended for API-driven or

³⁸ See [TCR Political Use Case Product Guide](#)

³⁹ See [CTIA Political Text Messaging](#) and CTIA's political messaging campaign resource at politicalmessaging.com.

⁴⁰ Some churches may not have a recognized 501(c)3 status but may still qualify for the Charity use case. See [TCR Small Church Registration as a 501\(c\)\(3\)](#) documentation for further guidance.

⁴¹ Accrediting organizations include [Better Business Bureau Wise Giving Alliance](#) and [Charity Navigator](#).

⁴² See [TCR Sole Proprietor Policy](#)

automated messaging. To register UCaaS campaigns, CSPs must complete an application process through TCR to obtain MNO approval. UCaaS Low Volume campaigns have restricted throughput and daily volume limits towards some carrier networks. Brands should consult with their connectivity partner to understand specific requirements related to UCaaS campaigns and refer to TCR documentation.⁴³

4.7.6 Platform Free Trial (PFT)

The PFT use case allows CSPs to support messaging for non-paying, time-limited trial customers. The CSP must restrict the sending of messages to up to ten opted-in numbers per trial participant and must cap PFT daily message volume and throughput as outlined in carrier policies. If the PFT campaign is associated with an ISV customer of the CSP, then the ISV must be listed as the reseller for the PFT campaign. Some MNOs require that message content is watermarked with the CSP or ISV name. To support this use case, CSPs must have a separate contract with TCR and submit a monthly report to TCR that covers their PFT activity.⁴⁴

4.8 Compliant Messaging Practices

4.8.1 Campaign Drift

Campaign drift, which refers to the gradual misalignment of a messaging campaign from its original goals, target audience, or messaging content over time, is not permitted. The actual message content sent from a campaign should not deviate from the originally declared use case, campaign description, and/or sample messages. Messages being sent or the overall purpose of the messaging program should accurately align with what was initially registered.

4.8.2 Embedded Links and Phone Numbers

Brands should ensure the responsible use of embedded website links and phone numbers in messaging content. The use of public URL shorteners (e.g. bitly, tinyurl, etc.) are not permitted in 10DLC message content. Brands should use branded or proprietary URL shorteners or links that demonstrate a relationship with the brand, reseller or CSP. Embedded phone numbers, excluding within the HELP response message, should be used judiciously and align with the campaign's purpose. All links and phone numbers should lead to relevant and secure destinations. The brand must specify whether messages will include embedded links or phone numbers by selecting the corresponding content attribute during the campaign registration process.

4.8.3 Message Frequency and Timing

Message frequency must be disclosed during the opt-in process, and campaigns must send messages at a reasonable frequency, respecting consumer preferences and avoiding excessive messaging or disruptive practices. Messages must be sent at a reasonable time, which includes respecting quiet hours by avoiding message delivery during those times.

⁴³ See [TCR UCaaS Use Case Documentation](#)

⁴⁴ See [TCR Platform Free Trial Product Guide](#)

A single opt-in confirmation message must be sent after a consumer opts into a 10DLC campaign, except for message programs using a double opt-in approach, in which case multiple messages may be sent. For opt-ins obtained outside the messaging channel, such as at a point of sale (POS) or via a hardcopy form, the opt-in confirmation message must be delivered as soon as reasonably possible after the user opts in.

4.8.4 Message Throughput

Message throughput refers to the volume or rate of messages that can be transmitted within a specific time frame, and can vary based on the carrier, the brand's vetting status, and the campaign use case. Generally, 10DLC message throughput is not allocated at the number level. Instead, some carriers allocate throughput per campaign, whereas other carriers assign a daily message volume allowance at the brand level, called brand tier. Brand tier is a system of daily volumetric caps, allocated to all campaigns associated with a particular brand. Some MNOs prioritize throughput for vetted brands, brands on the Russell 3000 stock market index, or specific use cases to ensure a higher quality of service.

Brands must manage throughput by understanding that it is allocated based on brand vetting status and campaign use case, not the quantity of numbers associated with the campaign. Brands should consult with their connectivity partner to ensure adherence to daily message volume or throughput limitations as specified by MNOs for the declared campaign use case.

4.8.5 Snowshoe Messaging

Snowshoe messaging is the disallowed practice of spreading messages across many phone numbers or 10DLC campaigns with the intention of circumventing message filters or avoiding volume restrictions. Campaigns may be rejected if content appears duplicated, indicating snowshoeing. Messages may be blocked or traffic may be suspended if snowshoe messaging is detected. Campaigns operating with an approved number pool are not considered as engaging in snowshoe messaging.

4.8.6 Message Content Monitoring

Participants within the 10DLC ecosystem must use best efforts to prevent and combat unwanted or unlawful messaging traffic, including spam and brand spoofing. They must take affirmative steps and employ tools that can monitor and prevent unwanted messages and content, including content that is unlawful, harmful, abusive, malicious, misleading, harassing, excessively violent, or defamatory. They must also ensure that links to websites embedded within a message do not conceal or obscure the brand's identity and are not intended to cause harm or deceive consumers.

4.8.7 Messaging Security

Participants within the 10DLC ecosystem must implement security measures to protect consumer data and prevent unauthorized access. This includes using strong passwords and multi-factor authentication to reduce the risk of account takeover and implementing authentication protocols for

API access and campaign management. Message senders must regularly monitor and update security measures to address potential vulnerabilities.⁴⁵

5. Appendix

5.1 Example Messages and Call-to-Actions

This section provides examples of messages and call-to-actions to help illustrate the required compliance components of 10DLC message programs.

5.1.2 Example Message Templates

Example Opt-in Confirmation Message (for recurring message programs)	
[Brand Name]: Welcome to [use case/program]. Reply HELP for help. Reply STOP to cancel. Msg frequency varies. Message and data rates may apply.	
Compliance Components	
Component	Description
Brand Name	Identifies the sender and matches the registered brand/DBA name
Confirmation of Opt-in	Confirms the user's opt-in to the specific message program
Message Frequency	Discloses how often the user can expect to receive messages
Opt-out Instructions	Informs the user how to opt out of the message program
Help Instructions	Informs the user how to get support from the brand related to the message program
Rate Disclosure	Includes the required disclosure "Message and data rates may apply"

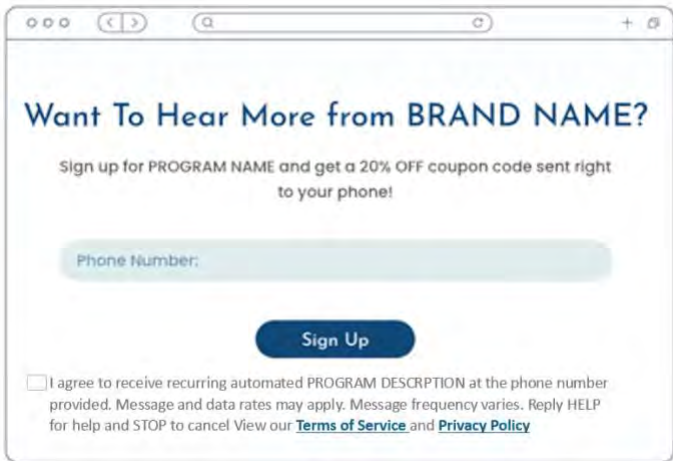
Example HELP Message	
[Brand Name]: For more information contact us at [brand email/brand phone number/brand website]	
Compliance Components	
Component	Description
Brand Name	Identifies the sender and matches the registered brand name
Help Instructions	Informs the user how to get support from the brand related to the message program

⁴⁵ See [CTIA Messaging Security Best Practices](#) for further guidance on messaging security best practices.

Example STOP Message	
[Brand Name]: You have been opted out; no further messages will be sent	
Compliance Components	
Component	Description
Brand Name	Identifies the sender and matches the registered brand/DBA name
Confirmation of Opt-out	Confirms that opt-out request has been processed and that the user will no longer receive messages

Example Content Messages	
<i>Example Marketing Campaign</i> [Brand Name]: Get 25% off all items this weekend only at [branded website link]. Shop now before it's too late! Reply STOP to cancel. <i>Example 2FA Campaign</i> [Brand Name]: Verification code for your login attempt: [XXXXXX]. This code will expire in 10 minutes. If you did not request this, please ignore this message.	
Compliance Components	
Component	Description
Brand Name	Identifies the sender and matches the registered brand/DBA name
Alignment with Use Case	Aligns with the registered use case and campaign description
Permitted Content	Avoids any disallowed content categories
Opt-out Instructions	Includes recommended opt-out instructions

5.1.3 Example Call-to-Actions

Example Web-Based Call-to-Action
 Want To Hear More from BRAND NAME? Sign up for PROGRAM NAME and get a 20% OFF coupon code sent right to your phone! Phone Number: Sign Up ☐ I agree to receive recurring automated PROGRAM DESCRIPTION at the phone number provided. Message and data rates may apply. Message frequency varies. Reply HELP for help and STOP to cancel View our Terms of Service and Privacy Policy

Compliance Components	
Component	Description
Consent Mechanism	The method by which the consumer provides consent is evident
Brand Name	Identifies the sender and matches the registered brand/DBA name
Program Description	Includes a description of the message program's purpose
Message Frequency	Discloses how often the user can expect to receive messages (required for recurring message programs only)
Opt-out Instructions	Includes opt-out instructions
Help Instructions	Informs the user how to get support from the brand related to the message program (not required if included in Terms and Conditions)
Rate Disclosure	Includes the required disclosure "Message and data rates may apply"
Link to Terms and Conditions	Includes a clear and conspicuous link to the complete terms and conditions of the messaging program (not required if full terms and conditions are included)
Link to Privacy Policy	Includes a readily accessible link to the privacy policy explaining how user information is collected, used, and shared (a declaration of privacy policy may also be acceptable)

Example Verbal Call-to-Action	
<i>Verbally [While On A Call/In Person/At POS]</i> "Would you like to receive [use case/program] messages from [Brand Name] via text? If so, please provide your mobile phone number to opt in. Message frequency will vary by account and preference. Message and data rates may apply. To opt-out, text STOP. Text HELP for more information. For terms and privacy, visit our website [brand website]."	
Compliance Components	
Component	Description
Consent Mechanism	The method by which the consumer provides consent is evident
Brand Name	Identifies the sender and matches the registered brand/DBA name
Program Description	Includes a description of the message program's purpose
Message Frequency	Discloses how often the user can expect to receive messages (recurring message programs only)
Opt-out Instructions	Includes opt-out instructions
Help Instructions	Informs the user how to get support from the brand related to the message program (not required if included in Terms and Conditions)
Rate Disclosure	Includes the required disclosure "Message and data rates may apply"

Example Verbal Call-to-Action	
Link to Terms and Conditions	Includes a clear and conspicuous link to the complete terms and conditions of the messaging program (not required if full terms and conditions are included)
Link to Privacy Policy	Includes a readily accessible link to the privacy policy explaining how user information is collected, used, and shared (a declaration of privacy policy may also be acceptable)

5.2 Additional Resources

This section provides a list of relevant industry resources and organizations for additional support and guidance.

5.2.1 Messaging and Compliance Resources

- [CTIA Messaging Principles and Best Practices](#)
- [CTIA Messaging Security Best Practices](#)
- [CTIA Political Text Messaging](#)
- [Privacy on the Go: Recommendations for the Mobile Ecosystem](#)
- [T-Mobile's Code of Conduct](#)

5.2.2 Regulatory Resources

- [Telephone Consumer Protection Act \(TCPA\)](#)
- [CAN-SPAM Act of 2003](#)
- [TCPA Omnibus Declaratory Ruling and Order](#)
- [Telemarketing Sales Rule](#)
- [Restrictions on Telemarketing, Telephone Solicitation, and Facsimile Advertising](#)
- [California Consumer Privacy Act \(CCPA\)](#)

5.2.3 Industry Organizations

- [The Campaign Registry](#)
- [CTIA – The Wireless Association](#)
- [Aegis Mobile](#)
- [WMC Global](#)
- [Campaign Verify](#)
- [netnumber](#)

5.2.3 The Campaign Registry (TCR) Resources

- [TCR Resources](#)