10DLC Messaging: Definition, History, and Industry Overview

By ClearlyIP Published April 28, 2025 55 min read

10DLC Messaging: Definition, History, and Comprehensive Industry Overview

Introduction

10DLC (10-Digit Long Code) refers to the use of standard 10-digit phone numbers for business text messaging in the United States. Unlike traditional person-to-person (P2P) texting, 10DLC is a carrier-sanctioned **application-to-person (A2P)** messaging channel that enables businesses to send SMS/MMS over local-looking numbers at higher volumes and with better reliability (Source:

support.telnyx.com)(Source: support.telnyx.com). This system was introduced as a solution to the growing problem of spam and unsanctioned marketing texts: by requiring registration and vetting of business senders, carriers can protect consumers from unwanted messages (Source: support.telnyx.com)(Source: 10dlc.org). Today, 10DLC messaging is a cornerstone of U.S. business texting, governed by industry guidelines and registration processes that ensure compliance and maintain trust in the messaging ecosystem.

Definition and History of 10DLC Messaging

Definition: 10DLC stands for *10-Digit Long Code*, meaning a standard ten-digit telephone number (in the North American Numbering Plan) used for A2P messaging (Source: support.telnyx.com). In practice, a 10DLC number looks like a normal local phone number (e.g. 212-555-0123) but is registered for business texting. This channel combines the familiarity of local numbers with carrier-approved throughput and compliance measures, making it a popular choice for organizations to send texts for marketing, alerts, two-factor authentication, customer service, and more (Source: support.telnyx.com).

Historical Background: In the early years of SMS marketing (2000s), businesses largely relied on *short codes* – 5 or 6-digit numbers – to send high-volume texts (Source: charlestontelecomsolutions.com). Short codes were effective but expensive and limited in availability, and many smaller businesses instead turned to regular long-code phone numbers (intended for P2P texting) to send texts in bulk (Source: charlestontelecomsolutions.com)(Source: tjthinakaran.blog). By the mid-2010s, A2P messaging via long codes had "boomed" in usage despite not being officially sanctioned by carriers (Source: tjthinakaran.blog). This unsupervised growth led to problems: carriers' SMS networks could not distinguish legitimate A2P traffic from person-to-person texts, resulting in spam and fraud slipping through P2P routes (Source: tjthinakaran.blog). Carriers treated unrecognized high-volume long-code traffic as spam attacks and applied content filtering and volume throttling, but the fundamental challenge was the lack of an A2P-specific long code system (Source: tjthinakaran.blog).

To address these issues, U.S. carriers collaborated on a new framework. In 2017, AT&T and partners ran a pilot that involved "tagging" messages with information about the sender's identity and campaign, proving that it was technically possible to differentiate A2P from P2P texts by using a campaign identifier in the message payload (Source: tjthinakaran.blog)(Source: tjthinakaran.blog). Following these trials, the wireless industry introduced **A2P 10DLC** as an official channel around 2018–2020 (Source: tjthinakaran.blog). Major carriers began rolling out 10DLC programs that would

require businesses to register who they are (Brand) and what types of messages they are sending (Campaign) before allowing large-scale texting on long codes. As part of this rollout, carriers also started phasing out **shared short codes** (short codes used by multiple brands), which were viewed as a source of spam. In fact, the top U.S. mobile operators *banned shared short codes in June 2021*, forcing businesses to migrate to dedicated 10DLC numbers or their own dedicated short codes (Source: truedialog.com). By October 2021, carriers fully enforced the new registration requirement: any business sending A2P messages via long code had to register their campaigns through the sanctioned system (or risk heavy filtering/blocking) (Source: truedialog.com).

Since then, 10DLC messaging has become the standard protocol for business texting in the U.S. (Source: tsgglobal.com). The industry's focus has shifted to refining the compliance and vetting processes. Over time, carriers and regulators (in partnership with a central registry, discussed below) have **expanded and refined 10DLC requirements** – introducing stricter compliance rules, more nuanced vetting (including trust scoring of message senders), and streamlined registration tools (Source: charlestontelecomsolutions.com)(Source: charlestontelecomsolutions.com). These efforts reflect an ongoing evolution aimed at balancing the needs of businesses (high deliverability and scale) with protection of consumers from spam or abusive messages (Source: charlestontelecomsolutions.com)(Source: charlestontelecomsolutions.com). In summary, 10DLC messaging emerged as a direct response to the challenges of the earlier SMS marketing era, providing a more controlled, trustworthy framework that continues to adapt to new messaging trends and threats.

Regulatory and Compliance Landscape

A2P 10DLC messaging in the U.S. operates within a tightly governed compliance landscape shaped by industry bodies, carriers, and a central registry. This framework is designed to ensure that businesses texting consumers adhere to best practices, legal requirements, and carrier policies.

- **CTIA Guidelines:** The Cellular Telecommunications Industry Association (CTIA) publishes industry guidelines for messaging, which, while voluntary, are widely adopted as best practices. The CTIA's *Messaging Principles and Best Practices* (most recently updated in 2023) emphasize consumer protection – requiring clear consent (opt-in) for any A2P messaging, honoring opt-out requests, and prohibiting content that is fraudulent or illegal (Source: 10dlc.org). Under these guidelines, all marketing, promotional, or informational texts from businesses must be permission-based. Messages should include or support standard keywords like STOP for opting out, and programs must avoid forbidden content categories (often

summarized by the CTIA's "SHAFT" rule: sex, hate, alcohol, firearms, tobacco are disallowed in marketing texts) (Source: support.bandwidth.com). The CTIA also operates a monitoring program (formerly for short codes, now applied to all A2P channels) that can audit or flag non-compliant campaigns. Though CTIA guidelines are not law, carriers enforce many of these principles on their networks, making compliance essential for any 10DLC campaign.

- **Mobile Carrier Policies:** Each major U.S. mobile carrier (AT&T, Verizon, T-Mobile, and others) has its own code of conduct and rules for A2P messaging, which build upon the CTIA guidelines and add carrier-specific requirements. For example, **T-Mobile's Code of Conduct** explicitly forbids certain practices and imposes hefty fines for violations – such as a $10,000 fee for serious spam or content violations and $10 per message for sending A2P traffic over P2P routes ("grey routing") (Source: support.bandwidth.com)(Source: support.bandwidth.com). AT&T and T-Mobile both announced in 2021 that they would no longer permit shared short code usage, aligning with the shift to 10DLC (Source: truedialog.com). To use 10DLC, carriers require that each business (Brand) and messaging use-case (Campaign) be registered in their systems via the official registry (The Campaign Registry). **Carriers also individually review campaign registrations** as part of the onboarding – it is an "industry-wide mandatory step" that each campaign submission gets vetted for compliance by the carriers (e.g., to ensure the content aligns with the declared use-case and that the business is legitimate) (Source: support.telnyx.com). Only approved campaigns are then allowed to send traffic. Each carrier reserves the right to suspend or filter messages that violate their policies even after approval, so ongoing compliance (maintaining good sending practices, not exceeding throughput limits, etc.) is crucial.

- **The Campaign Registry (TCR):** A central component of the 10DLC ecosystem is *The Campaign Registry*, often called **TCR**, which is a third-party entity serving as the **"central hub" for registering A2P 10DLC campaigns** (Source: statevoices.org). TCR is essentially a database and verification service: Businesses (Brands) cannot directly register themselves with TCR; instead, the registration is handled by **Campaign Service Providers (CSPs)** – these are messaging providers or aggregators (like Twilio, Bandwidth, Telnyx, etc.) who interface with TCR (Source: campaignregistry.com). When a business wants to use 10DLC, the CSP collects their information and submits a *Brand registration* (company details, industry, etc.) and *Campaign registration* (description of the messaging program, use-case, sample messages, etc.) into the TCR system. TCR verifies the Brand's identity (and may perform additional vetting via third parties for a "Trust Score", explained later) and records the Campaign details. The **10DLC messaging ecosystem relies on TCR as the backbone** – it provides a *sanctioned, verified environment* where "Brands, CSPs, and messaging content are all known upfront," making the origin and purpose of each message traceable (Source: campaignregistry.com)

(Source: campaignregistry.com). Essentially, TCR acts as the gatekeeper: only registered and approved campaigns are allowed by carriers, and TCR's data feeds into carriers' systems so they know who is sending a given message. This traceability and verification step was introduced to bring accountability to long code messaging, which previously was opaque. The **Campaign Registry was launched in 2020** as carriers transitioned to 10DLC requirements, and by late 2021 it became a mandatory step for all A2P long code messaging (Source: truedialog.com).

In addition to these, federal regulations like the **Telephone Consumer Protection Act (TCPA)** underpin the legal side of text messaging consent in the U.S. (e.g. requiring express consent for marketing texts, with significant penalties for non-compliance). While TCPA enforcement is outside the scope of carriers/TCR, the 10DLC framework is designed to help businesses stay compliant with such laws by enforcing upfront consent and opt-out mechanisms.

Technical Architecture and Messaging Workflow

The 10DLC messaging workflow involves multiple players and technical steps to ensure that each message sent by a business is authorized and compliant:

- **Key Players in the Ecosystem:** According to industry documentation, the main entities in a 10DLC message flow include: **Brands** (the business sender), **CSPs** (Campaign Service Providers, essentially messaging platforms or API providers that register campaigns and send messages on behalf of brands), **Aggregators or DCAs** (Direct Connect Aggregators, companies with direct carrier connections that often handle message throughput and campaign approvals for the carriers), **Mobile Network Operators** (the wireless carriers themselves, like AT&T, Verizon, T-Mobile), and **TCR** (The Campaign Registry, which sits in the middle as the reputation and registration database) (Source: telgorithm.com)(Source: telgorithm.com). In simpler terms, when a business wants to send a text blast via 10DLC, it does so through a CSP (for example, a cloud communications platform), which in turn coordinates with TCR and the carriers to make sure the campaign is registered and the messages are appropriately routed.

- **Registration and Provisioning:** Before any significant messaging can occur, a *Brand* and *Campaign* must be registered (as detailed in the next section). Once a campaign is approved, it is assigned a unique **Campaign ID** in the TCR system. The CSP associates one or more 10DLC phone numbers to that campaign. Technically, when messages are sent, the Campaign ID and other metadata are used behind the scenes (for example, in the message protocol or routing information) to inform carriers which campaign the message belongs to. The Campaign Registry

notes that *"messages are sent soon after the Campaign Registry user provides their connectivity partner with a Campaign ID"*, indicating that once a campaign is registered and provisioned by the CSP, messaging can commence without lengthy delays (Source: campaignregistry.com).

- **Message Flow:** The actual path of a 10DLC message typically goes as follows: The business's application sends a text (via API) to the CSP's platform, specifying the 10DLC phone number as the sender. The CSP (who has the campaign approval on record) forwards the message through an aggregator or direct connection into the carrier networks. The message enters the carrier's A2P pipeline – which may involve the carrier checking the sending phone number and campaign against what's registered in their systems (to ensure this number is authorized for that type of campaign). Because the campaign and brand information is known upfront (via TCR data), carriers can apply any appropriate throughput limits or filtering in real time. The message then gets delivered to the end-user's mobile device via the carrier's infrastructure. If the end-user replies or sends a message to that 10DLC number, the reverse path carries it back to the business (note: 10DLC supports **two-way messaging**, so customers can respond to the texts, unlike some one-way short code programs).

- **Network and Architecture Considerations:** Under the hood, 10DLC messages travel over the same SMS/MMS protocols (like SMPP) but often over dedicated A2P routes that carriers have set up (separate from the P2P paths). In the legacy system, when carriers saw traffic coming from inter-carrier vendors (aggregators), they assumed it was P2P and treated it leniently (Source: tjthinakaran.blog). Now, with 10DLC, carriers use routing identifiers and source authentication to know it's A2P. AT&T's initial pilot introduced the idea of a *"message header" containing a campaign tag*, and indeed today AT&T still uses a form of message tagging to identify the campaign for each message on their network (Source: tjthinakaran.blog). Other carriers may use the originating phone number as a lookup key against a database of approved campaigns. The net effect is the same: every 10DLC message is linked to a registered campaign, allowing carriers to trace who sent it and what type of content it should be. This technical linkage also enables **auditability** and **traceability** — if spam or abuse is reported, carriers can quickly identify the source campaign/brand via TCR records.

- **Throughput and Filtering Technology:** In the 10DLC architecture, carriers enforce **throughput limits** (rate limits on messages) to each campaign/number as determined by the campaign's approval tier (see next section). For example, a carrier might allow a high-volume campaign to send, say, 50 messages per second, whereas a low-tier campaign might be limited to only 1 message per second. These limits can be implemented in the aggregator's software (queueing messages if they exceed the rate) and in the carrier's SMS gateways. If a campaign exceeds its

allowed rate or daily volume (in the case of T-Mobile), the extra messages will be queued or rejected until the window resets (Source: support.bandwidth.com)(Source: support.bandwidth.com). Carriers also have content filters (automated systems scanning for prohibited content or spam patterns) and may utilize third-party *spam detection* algorithms (often provided by firewall companies like Proofpoint/Cloudmark or AdaptiveMobile) to monitor 10DLC traffic. However, registering and vetting the campaign significantly lowers the chance of filtering, since the carrier *knows* the traffic is sanctioned. Indeed, one of the selling points of 10DLC is **improved deliverability compared to unregistered long codes**, because legitimate traffic is less likely to be erroneously blocked (Source: support.telnyx.com).

In summary, the 10DLC technical workflow adds an overlay of identity and enforcement on top of the existing SMS network. By integrating TCR's registry information with carrier routing and filtering systems, 10DLC ensures that when a business text message is sent, the carriers have confidence about *who* is sending it and *what* it's about, enabling higher volumes and reliability while keeping bad actors out.

Differences Between 10DLC, Short Codes, and Toll-Free Messaging

In the U.S., A2P messaging can be sent via several types of sender identifiers: **10DLC long codes**, **short codes**, and **toll-free numbers**. Each has distinct characteristics, advantages, and limitations. The choice often depends on a business's specific needs (scale, cost, branding, etc.). Below is a comparison of these three:

- **Number Format & Recognition:** *Short codes* are 5-6 digit numbers (e.g. 12345) dedicated to A2P messaging. They are highly recognizable and easy for consumers to remember, which is beneficial for marketing campaigns and one-to-many alerts (Source: infobip.com)(Source: infobip.com). *10DLC* numbers, by contrast, look like ordinary phone numbers (10 digits). While they aren't as instantly identified as business senders, they can appear more personal or local (e.g., a message from a local area code may feel like it's from a local business). *Toll-free numbers* (e.g. 1-800 or 1-888 numbers) are another format – these have a special three-digit prefix and traditionally were used for voice calls where the business pays the cost. Toll-free numbers can be SMS-enabled for A2P use; they are somewhat recognizable as business lines due to the 800-type prefix, and they convey a national presence.

- **Setup Process and Speed:** Obtaining a short code involves a **lengthy provisioning process**. Businesses must lease the short code (often at significant cost) and get carrier approvals for their campaign content, which can take several weeks to complete due to rigorous vetting (Source: infobip.com). In contrast, 10DLC numbers are **much quicker to deploy**. Because they are regular phone numbers, a business can acquire a number almost instantly from a provider. The main time investment is the registration with TCR, which, depending on the provider and vetting, can be done in days (and in some cases is automated to be near-immediate for standard campaigns). Toll-free numbers fall in between: getting a toll-free number is quick, but **toll-free verification** (an optional but recommended process to whitelist the number for high-volume A2P messaging) can take a week or more for carriers to approve. Overall, if time-to-launch is critical, 10DLC and toll-free generally allow faster onboarding than short codes (Source: infobip.com)(Source: infobip.com).

- **Cost Structure:** Short codes carry the **highest cost**. Leasing a vanity or random short code can range from $500 to $1,500 *per month*, not including messaging fees. This premium reflects the high throughput and exclusive nature of short codes. 10DLC numbers, on the other hand, are inexpensive to obtain – typically just the cost of a normal phone line (a few dollars per month at most), plus the 10DLC registration fees. The **registration fees for 10DLC** include a one-time Brand registration fee (around $4 for a standard business, although some providers charge around $40 which includes extra vetting) and a Campaign registration fee (around $10 per campaign) (Source: support.telnyx.com)(Source: support.telnyx.com). Additionally, there's a monthly campaign fee of $2 to $10 depending on the campaign type (Source: support.telnyx.com). Carriers also impose per-message fees (surcharges) on 10DLC traffic (see next section for details). Toll-free numbers have **moderate costs**: typically a small monthly fee for the number (e.g. $1-$5/month) and no extra per-message surcharge from carriers (as of now, toll-free messaging has its own fee regime separate from 10DLC, though some carriers recently introduced a minimal fee for toll-free as well (Source: telgorithm.com)). In summary, 10DLC is attractive for its low setup and monthly costs compared to short codes (Source: infobip.com), making it accessible to businesses of all sizes. Toll-free lies in the middle, cheaper than short codes, but generally a bit more expensive per message than 10DLC (toll-free SMS usually costs slightly more in messaging provider fees, and if not verified, can be heavily filtered).

- **Throughput and Volume:** Short codes are king in throughput – they were designed for **mass texting** and can send hundreds of messages per second (in many cases 100+ MPS by default, and scalable much higher for large programs). They also have no daily caps; you can send millions of messages per day on a short code if approved. 10DLC numbers, due to the

regulations, have **rate limits** based on the campaign's trust score and use-case. A single 10DLC campaign's throughput might range from as low as 1 message per second (for an unvetted small brand) up to perhaps 50+ messages per second for a top-tier fully vetted campaign – we'll detail exact limits in the next section. Also, T-Mobile imposes a **daily message cap** per brand on 10DLC (e.g., typically 2,000 messages/day for a new low-tier brand, up to 200,000/day for a high-trust brand) (Source: support.bandwidth.com)(Source: support.bandwidth.com). This means 10DLC is suitable for moderate volumes but not massive blasts in a short time. Toll-free numbers generally have high throughput potential – many carriers allow toll-free SMS to achieve around 30 MPS or more, and there are no explicit daily caps. One advantage of toll-free is that it can sometimes match or exceed 10DLC throughput without the need for the same detailed registration; however, toll-free traffic is subject to carriers' **spam filtering and a vetting process** as well (businesses are encouraged to submit a verification form to carriers to ensure high throughput and deliverability for toll-free). In practice, for extremely high-volume use-cases (like voting campaigns, big retail flash sales), *dedicated short codes* remain the best option due to their reliability at scale. For mid-volume, regional, or two-way conversational use-cases, *10DLC* is usually ideal. Toll-free is often used for customer support lines or nationwide brands that prefer one number for voice and text, handling mid-to-high volumes once verified.

- **Use Case Suitability:** *Short codes* are ideal for **large marketing campaigns, one-to-many alerts**, and any scenario where a memorable number or maximum throughput is needed (e.g. SMS blasts to millions for a product launch, emergency alerts, or big national campaigns). They are less personal (clearly a marketing channel) and are typically one-way or high-level two-way (you often see automated responses on short codes). *10DLC* shines for **localized or personalized campaigns** and **conversational messaging**. Because they look like regular numbers, 10DLCs are great when you want customers to engage in a back-and-forth conversation – for instance, a sales rep texting a client, or an appointment reminder that allows the customer to reply to confirm or reschedule. They are also well-suited for regional marketing (sending from a local area code to increase trust). *Toll-free numbers* are often used by **national brands and support lines** – for example, a company might use one toll-free number as a text-enabled customer support channel across the country. Toll-free SMS can handle both one-way blasts and two-way interactions, but the branding is less local than 10DLC (more corporate/national feel). It's worth noting that **certain programs can only be done on specific channels**: for instance, **"free-to-end-user" (FTEU) messages** (where the consumer isn't charged, often used by charities or healthcare) are only supported via specially provisioned short codes, not via 10DLC or toll-free (Source: support.telnyx.com). Likewise, *handset delivery*

receipts (true confirmation that a message reached a phone) are generally available on short codes and toll-free, but not on 10DLC (on 10DLC you usually get network-level delivery confirmation) (Source: support.telnyx.com).

Below is a **summary comparison table** highlighting key differences:

FEATURE/CRITERIA	10DLC (LOCAL LONG CODE)	SHORT CODE (5-6 DIGIT)	TOLL-FREE NUMBER (TEXT-ENABLED 8XX)
Typical Throughput	Tiered by campaign Trust Score; e.g. 1–50 MPS (approx). Daily cap (T-Mobile: 2k–200k/day) (Source: support.bandwidth.com). Higher trust can reach ~200+ MPS across carriers (Source: callhub.io) (Source: callhub.io), but generally lower than short code.	Very high throughput (100+ MPS easily; can scale to thousands of TPS). No set daily cap. Best for mass volumes.	Moderate to high (typically 25–50 MPS once verified). No formal daily cap, but heavy unverified traffic can be filtered.
Setup Time	Quick (days). Requires Brand/Campaign registration via TCR, but number procurement is instant.	Slow (weeks). Lease code and get carrier approvals for campaign content in advance.	Moderate (days to ~1 week). Number purchase is instant; optional carrier verification process for high volume.
Cost	Low setup cost. Number ~$1/month. Registration: ~$4 Brand + ~$10 Campaign one-time, plus $2–$10/month per campaign (Source: support.telnyx.com) (Source: support.telnyx.com). Carrier per-message fees ~$0.002–$0.003 each (SMS) (Source: redoxygen.com).	High cost. Short code leasing $500–$1000+/month. One-time setup fees possible. Messaging costs per SMS similar to standard rates but no extra surcharges (already premium pricing).	Moderate cost. Number $1–$5/month. No per-message surcharge from carriers (aside from normal messaging fees), though some carriers introduced small toll-free fees (e.g. AT&T ~$0.003 inbound) (Source: telgorithm.com).

FEATURE/CRITERIA	10DLC (LOCAL LONG CODE)	SHORT CODE (5-6 DIGIT)	TOLL-FREE NUMBER (TEXT-ENABLED 8XX)
Use Case Examples	Two-way customer conversations, localized promotions (e.g. a clinic texting patients from a local number), app notifications, marketing where a personal touch helps. Supports both low and fairly high volume use cases.	Large marketing campaigns (e.g. text-to-vote, nationwide alerts), time-sensitive OTP (one-time passcodes) at massive scale, brand short codes for easy recognition (e.g. “Text SAVE to 12345”). Generally one-to-many scenarios.	National customer service or sales line (one number advertised for texting), broad opt-in campaigns where a single national number is acceptable (e.g. SMS support for a nationwide retail chain). Often used when voice calls on the same number are also offered.
Regulatory/Compliance	Must register via The Campaign Registry. Each campaign tied to specific use-case and content; non-compliance or unregistered traffic subject to blocking and fines (Source: support.bandwidth.com) (Source: support.telnyx.com). No shared use (each number tied to one campaign).	Carrier approval acts as upfront compliance gate; content scrutinized in provisioning. Shared short codes (multiple brands on one code) are banned (Source: truedialog.com). Short codes expected to maintain high compliance or risk shutdown.	Requires following CTIA guidelines and (informally) a verification process for high volumes. Generally more lenient filtering than unregistered long codes, but spam/abuse on toll-free can lead to suspension.

Note: "MPS" = messages per second. "TPS/TPM" (transactions per second/minute) terminology varies by carrier.

Registration and Vetting Process (Brand, Campaign, Trust Scores, Throughput Tiers)

One of the defining features of 10DLC is its registration and vetting process, which every business must navigate before sending significant A2P traffic. This process involves **identifying who you are (Brand)**, **what messages you're sending (Campaign)**, and how trustworthy your organization is (via a **Trust Score**). The outcome of this process directly influences your messaging limits (throughput) and messaging costs. Below is a detailed breakdown of each component:

- **Brand Registration:** A *Brand* in 10DLC context represents the business or organization behind the messaging. When registering, you provide information such as your company name, address, country, EIN (Tax ID) if applicable, industry, etc. This data establishes your identity. Brands are categorized by type (for example, "Standard" brands are those with an EIN, while "Sole Proprietor" brands are very small senders without a formal EIN). The registration is typically done through your messaging provider's interface, which connects to The Campaign Registry. There is a one-time fee for registering a Brand (around $4 for a standard brand via TCR, although some CSPs charge more to include a vetting service) (Source: support.telnyx.com). Once a Brand is registered, it is assigned a unique Brand ID in TCR's system.
    - **Secondary Vetting & Trust Score:** For *Standard Brands* (those with a tax ID), there is an option (and often a necessity for better throughput) to undergo **secondary vetting**. This is an automated or manual review of the brand by a third-party reputation service (endorsed by TCR) that assesses the brand's legitimacy and messaging practices. The output is a **Trust Score**, a numeric score typically **0 to 100** indicating the level of trustworthiness (Source: callhub.io). A higher score means the brand is considered lower-risk and more reputable, which translates into higher messaging throughput allowances. Trust Scores are generally bucketed into ranges; for example, 0–49 = low trust, 50–74 = medium, 75–100 = high (Source: callhub.io). According to industry guidance, a score above 70 is "good," while 50 or below is "poor," and the very best brands might score 90+ (Source: callhub.io) (Source: callhub.io). The vetting algorithm may consider factors like the brand's industry, how long it's been in business, online presence, reported spam complaint history, etc. There is usually an extra fee for secondary vetting (often ~$40) unless bundled. If a brand

skips secondary vetting, it may receive a default low score (often 0 or 1) by default, which significantly limits throughput (Source: callhub.io)(Source: callhub.io). It's worth noting that certain special verified brands (like well-known large public companies) might automatically be assigned high trust by virtue of their status (Source: support.telnyx.com)(Source: support.telnyx.com) – for instance, the top U.S. stock index companies (Russell 3000) are often given high throughput by default on some carriers (Source: support.telnyx.com) (Source: support.telnyx.com).

  - **Sole Proprietor Brands:** For individuals or very small businesses without an EIN, the ecosystem provides a "Sole Proprietor" pathway. These do not receive a numeric Trust Score; instead, they are by default treated as low-volume senders with fixed small limits (Source: reddit.com). Sole Proprietor registration requires identity verification (often an OTP to the person's phone and other checks) (Source: telgorithm.com)(Source: telgorithm.com). There is typically a limit of one campaign and one phone number per sole proprietor brand (Source: telgorithm.com). The carriers impose strict throughput caps on this category – e.g. AT&T allows at most **15 messages per minute** and T-Mobile **1,000 messages per day** for sole proprietor campaigns (Source: telgorithm.com)(Source: telgorithm.com). These limits ensure that large-scale senders cannot pretend to be individuals to avoid vetting. If a sole proprietor needs to scale beyond these limits, they effectively must upgrade to a standard brand with an EIN and go through full vetting (Source: signalhouse.io).

- **Campaign Registration:** Once a brand is ready, the next step is to register a *Campaign*. A campaign defines a specific messaging use case or program that the business intends to run. During registration, you must select a **Campaign Use Case Type** from a list of standard options (examples include Marketing, Mixed, Two-Factor Authentication, Account Notifications, Customer Care, Political, Charity, etc.). Each use case has certain requirements and possible restrictions. You also provide a campaign description and example messages, detailing what content will be sent and how users opt in. The campaign is then submitted (with a fee, typically $10) for approval. **Carriers (via the DCA aggregators) review campaigns manually** as needed (Source: support.telnyx.com) – checking that the content aligns with the chosen category and that the campaign isn't likely to send spam.

  Campaigns are tied to one or more phone numbers: you assign your 10DLC number(s) to the campaign once it's approved. Notably, **one phone number cannot be used for multiple campaigns simultaneously** – it's one campaign per number (though one campaign can have many numbers) (Source: support.telnyx.com). This prevents content mixing; if you need a single

number to handle multiple types of messaging (e.g., both marketing and transactional alerts), you might choose a "Mixed" use case campaign which allows some blend (with typically lower throughput given the broader scope) (Source: support.telnyx.com).

Additionally, there are **Special Use Cases** that have their own rules – for example, *Political* campaigns (for U.S. federal elections) require verification via a 3rd-party like Campaign Verify and are allowed very high throughput but only for that specific purpose (Source: support.telnyx.com). *Charity* campaigns (registered 501(c)(3) non-profits) may have fee waivers or special throughput considerations – indeed, AT&T's policy shows no per-message fees for 501(c)(3) campaigns and relatively high limits (Source: redoxygen.com). *Emergency* services or *Public Safety* campaigns likewise get special high throughput and often fee exemptions (Source: redoxygen.com). Each special use case often needs pre-approval or extra documentation.

- **Throughput Tiers and Carrier-Specific Limits:** After registration, the combination of your **Trust Score and Campaign use case** will determine your allowed messaging throughput. This is where each carrier's policies come in:
    - **AT&T:** AT&T uses a system of **"Messaging Classes"** (often labeled A through X, etc.) to assign throughput. In essence, AT&T looks at your use case *and* your vetting score to slot your campaign into a throughput tier. For standard marketing or mixed campaigns, a high trust score (e.g. 75-100) might land you in Class A/B, which corresponds to **4,500 messages per minute** allowed (Source: support.telnyx.com). A mid-level trust (e.g. score 50-74) might be Class C/D with about **2,400 messages per minute** (Source: support.telnyx.com). Low trust (score 1-49) could be Class E/F, around **240 messages per minute** (Source: support.telnyx.com). And if you did not vet at all (score 0 or "Basic" small business), you might be Class T with a mere **75 TPM (transactions per minute)** (~1.25 per second) limit (Source: support.telnyx.com). AT&T also differentiates by content: certain special classes like political (Class K) get the top tier (4500 MPM) regardless (Source: support.telnyx.com)(Source: support.telnyx.com), whereas others like social media platforms have even higher limits (there's a class for large social apps at 60,000 MPM per campaign) (Source: redoxygen.com). The message here is that AT&T's throughput is *granularly assigned based on campaign type and trust*. The highest throughput on 10DLC (thousands per minute) is attainable only for well-vetted, high-trust campaigns, and typically those are large businesses or critical services. A small new marketer will start at a much lower allowed rate, but can improve it by raising their trust score via vetting.

- **T-Mobile:** T-Mobile takes a different approach – it enforces a **Daily messaging cap** per brand (across all campaigns for that brand). T-Mobile's system assigns each brand a "Brand Tier" that maps to a daily limit. By default, a new registered brand without vetting is often in the *Low tier*, which is **2,000 messages per day** to T-Mobile (including Sprint) subscribers (Source: support.bandwidth.com)(Source: support.bandwidth.com). If the brand gets a higher trust score through vetting, the cap increases: e.g. **10,000/day** for a medium tier (score 25-49), **40,000/day** for upper-mid (50-74), and up to **200,000 per day** for high (75-100) (Source: support.bandwidth.com). Some large reputable brands may start at 200k by default (T-Mobile "High-Performance" default tier) (Source: support.bandwidth.com). These daily buckets are shared by all campaigns under the same brand/EIN on T-Mobile's network, which means if you have multiple campaigns or use multiple providers, all those messages add up to the one daily cap (Source: support.bandwidth.com)(Source: support.bandwidth.com). If you hit the cap, T-Mobile will queue the messages and deliver them the next day (or the provider may hold them) (Source: support.bandwidth.com). For brands that need to exceed 200k/day, T-Mobile offers a **Special Business Review (SBR)** process to request higher limits (potentially millions/day), which involves a fee and additional vetting – currently T-Mobile has a $5,000 fee listed for SBR, though it's waived until further notice (Source: support.telnyx.com). In terms of per-second throughput, T-Mobile doesn't explicitly publish an MPS, but the daily cap effectively controls volume. For example, 2000/day is roughly ~1.4 messages per minute on average if spread out (so clearly a low-tier cap will throttle heavy bursts significantly).

- **Verizon:** Verizon has been less transparent in public about how it assigns throughput. Officially, Verizon has not published detailed tiers or required scores (Source: telnyx.com). However, many sources indicate that Verizon's system allows quite generous throughput for 10DLC. A commonly cited figure is about **6,000 messages per minute per campaign** as an upper limit for Verizon (Source: redoxygen.com) (which equals 100 messages per second, likely sufficient for most use cases). Verizon seems to treat all approved 10DLC campaigns similarly, without the complex tiering that AT&T and T-Mobile use, though it undoubtedly monitors sender reputation. In practice, if you are registered and not sending spam, Verizon will deliver at high rates up to their implicit cap. The lack of transparency means businesses have to follow general best practices and ensure compliance, as Verizon might silently throttle or filter if it detects issues, but you won't get an explicit "cap number" from Verizon beyond broad guidance from your provider.

- **Other carriers:** Smaller U.S. carriers (e.g. US Cellular and various regional/mobile virtual network operators) also honor the 10DLC registrations. They typically don't impose additional strict caps beyond what's set by the primary data (and their traffic volumes are smaller). Often they are grouped as "minor carriers" in throughput tables. For instance, one guideline suggested minor carriers collectively might allow something like 75 MPS in total for high trust campaigns (Source: callhub.io) (as compared to 225 MPS across the big three combined) – but this is largely handled by the messaging providers automatically, and the exact limits are rarely hit in practice due to the distribution of users.

It's useful to illustrate throughput with an example: a **Standard Brand** that underwent vetting and scored, say, 85 (High Trust) registers a *Marketing campaign*. On AT&T, that campaign might be Class A with ~4500 TPM (~75 TPS) allowed (Source: support.telnyx.com). On T-Mobile, the brand would be allowed up to 200k messages/day (Source: support.bandwidth.com) (which is plenty for many campaigns; if they tried to send all 200k in one hour, that's ~55 TPS, which T-Mobile might allow in bursts as long as daily total is not exceeded). On Verizon, that campaign could likely send up to ~100 TPS without trouble (Source: redoxygen.com). In aggregate, the CSP might advertise this as, for example, "up to 225 messages per second across major networks" – which matches the Twilio guidance for top-tier brands (225 MPS total across AT&T, T-Mobile, Verizon) (Source: callhub.io). Conversely, a *low-trust or unvetted* brand might be limited to perhaps 1-5 TPS on each carrier, which could severely slow down a large send (and as noted, a sole proprietor brand is capped at 15 messages *per minute* on AT&T (Source: telgorithm.com) and 2,000/day on T-Mobile (Source: support.bandwidth.com), which is very low). This tiered system encourages senders to verify their identity and maintain good practices to earn higher throughput.

- **Post-Registration Monitoring:** Even after getting an approved campaign and initial throughput assignment, the vetting isn't "one and done." Carriers continuously monitor traffic for spam or anomalous behavior. The **Trust Score** could be adjusted or overridden if a sender generates complaints or violates rules. Campaigns can be suspended by carriers if they start hitting spam traps or if unwanted traffic is reported. Furthermore, The Campaign Registry can impose additional checks – for example, CSPs must report the monthly message volumes for any Sole Proprietor brands to TCR (Source: telgorithm.com), and there are limits on how many brands or campaigns can be associated with the same entity to prevent abuse (like one person creating dozens of "sole proprietor" brands; TCR limits each phone or email to a certain number of such registrations) (Source: telgorithm.com). All these measures ensure the 10DLC ecosystem remains healthy and that high throughput privileges are only used by reputable senders.

Use Cases and Real-World Applications

10DLC messaging is used across industries and for a wide variety of applications. Here are some of the most common use cases, along with real-world examples:

- **Marketing and Promotions:** Businesses use 10DLC to send marketing campaigns, promotions, and coupons to customers who have opted in. For instance, a local retail store might text out weekly discount codes to its subscriber list using a 10DLC number with the same area code, making the message feel local and personal. Restaurants could send daily specials or holiday offers to their customer base. Because 10DLC supports two-way messaging, customers might respond with questions or requests (e.g. "Text back STOP to unsubscribe, or ASK for more info"). *Example:* A fitness gym franchise sends a text blast: "**New Year Promo**: Get 50% off your first month! Show this text at any of our locations. Reply HELP for more info or STOP to opt out."

- **Alerts and Notifications:** A huge category of 10DLC traffic is operational or informational alerts. This includes appointment reminders (doctors, salons, vet clinics reminding you of upcoming appointments), shipping and delivery notifications (your package tracking updates), bank alerts or fraud warnings, flight status updates from airlines, and school/university notifications. These messages are often time-sensitive and expected by the user. *Example:* A dental office sends a reminder: "Hi [Name], you have a cleaning appointment on Jan 10 at 3:00 PM. Reply C to confirm or R to reschedule." Another example: a bank uses 10DLC to send a low-balance alert or a one-time passcode for login (though one-time passcodes (2FA) can also be on short codes, smaller services often just use 10DLC).

- **Two-Factor Authentication (2FA) and Security:** While many large internet companies use short codes for 2FA, smaller services or internal systems might employ 10DLC to send one-time PIN codes or login links. For moderate volumes (say a few hundred codes per day), 10DLC is sufficient and quick to set up. *Example:* A company's VPN system texts employees a verification code from a 10DLC number when they log in from a new device.

- **Customer Service and Conversational Messaging:** One of the strengths of long codes (10DLC) is that they support conversational flows naturally (just like a normal phone number texting). Businesses have embraced this for customer support via text. For example, a customer could text a help line number (which is a 10DLC) saying "I need help with my order #12345," and a support agent (or AI bot) can respond and have a back-and-forth conversation on that thread. This is common in industries like e-commerce (text-based order support), healthcare (patient texting a clinic), education (students texting questions to admissions), and more. *Example:* An

insurance agent gives out their dedicated 10DLC number so clients can text in photos of minor car accident damage and get guidance on claims – it's a personalized channel that still goes through an official system.

- **Emergency and Alerts (Public Sector):** Municipal or local government alerts (e.g., city notices, school district alerts) can use 10DLC numbers. For true mass emergency notifications, short codes or FEMA systems are used, but for more routine public service announcements (street cleaning reminders, utility outage notices, COVID vaccination clinic info) a city may use a 10DLC number. Nonprofits also use 10DLC for community outreach texts or fundraising campaigns (if 501(c)(3), often under the special Charity use case which can lower costs). *Example:* A non-profit community center might text "Reminder: Free workshop on job training tomorrow at 5 PM. Reply YES to RSVP."

- **Political Campaigning:** Political organizations (for example, campaign offices for candidates or advocacy groups) use 10DLC to send texts to voters – for event invites, get-out-the-vote reminders, donation drives, etc. Political use cases are special: federal campaign texts must go through a verification (Campaign Verify) and are treated as their own class under 10DLC with typically high throughput to accommodate surges near elections (Source: support.telnyx.com). In recent U.S. elections, texting has been huge; while some campaigns still attempt peer-to-peer texting from individual phones to bypass A2P rules, the major carriers and TCR now encourage formal registration of political texts as 10DLC campaigns for transparency and control. *Example:* A registered political 10DLC campaign might send: "Hi, it's Maya from XYZ Campaign. Election Day is Nov 8. Can we count on your vote? Find your polling place: [link]. Reply YES/NO."

- **One-Number-to-Many Agents (Franchise use):** Some organizations with multiple agents or outlets (real estate offices, ride-share driver communication, etc.) may use unique campaigns to allow each agent to have their own local number but still register under a broader use case. For example, a large real estate company could register a special "franchise/agent" use case (some carriers had a class for this) that permits many numbers (one per agent) under the company brand. This way each agent texts clients from a distinct number, but all follow the same compliance template. The 10DLC framework has support for such scenarios (with certain classes like the "Agents and franchises" campaign type under AT&T's special classes (Source: redoxygen.com)).

- **Internal Business Communications / Workforce Messaging:** Although 10DLC is primarily about A2P (business-to-consumer), some companies use texting to communicate with employees or field workers (e.g., schedules, alerts). If those messages are sent en masse, they

still fall under A2P and thus need 10DLC registration (often as an "alerts" or "staff notification" use case). For instance, a hospital might blast an SMS to all staff for an urgent meeting. This would be registered likely as an "Emergency" or "Staff Alert" campaign.

These examples demonstrate the versatility of 10DLC. The common theme is that all such use cases require *prior express consent* from recipients. Whether it's a simple "Text me if my table is ready" or opting into a coupon program, the subscriber must agree to receive these texts (per CTIA and carrier rules). The Campaign Registry process forces businesses to declare that they've obtained the proper consent for the type of campaign they register, and carriers can demand proof if there's a complaint. This has made **opt-in list building** an important part of any text campaign strategy in the 10DLC era. For real-world success, organizations have to not only use the right channel for the right message but also maintain compliance and good sending practices (like including your business name in messages, providing clear opt-out instructions, and not blasting at odd hours). When done right, 10DLC messaging has very high engagement – as SMS boasts open rates around 98% (Source: truedialog.com) – and thus is a powerful tool for customer communication.

Pros and Cons of 10DLC Messaging

When evaluating 10DLC as a messaging solution, it's important to weigh its advantages and disadvantages, especially in comparison to alternatives (like short codes or toll-free). Below are key pros and cons of the 10DLC framework:

Pros:

- **Local & Personalized Branding:** 10DLC numbers allow businesses to use *local area codes*, which can make messages feel more personal and geographically targeted. Customers are often more likely to trust or open a text from what looks like a familiar local number versus a short code or a random toll-free (Source: reddit.com). This is great for local businesses or any brand that wants to appear local to different markets by using different area codes.

- **Lower Cost & Easier Access:** Compared to short codes, 10DLC is far more affordable and accessible. There are no exorbitant leasing fees – just nominal registration costs – and you can get started much faster (Source: infobip.com)(Source: infobip.com). This opens up high-volume texting capabilities to small and medium businesses that could never justify a short code. Even the ongoing per-message carrier fees for 10DLC (fractions of a penny per SMS) are relatively small, especially for registered traffic (Source: support.telnyx.com)(Source: support.telnyx.com).

- **Higher Throughput than Traditional Long Codes:** Before 10DLC, if a business tried to send texts over a normal phone number, carriers would heavily filter or rate-limit them (often to 1 message per second or less) and delivery was unreliable. With 10DLC, businesses get *sanctioned throughput* – significantly higher sends are possible, on par with many short code campaigns for well-vetted senders. And because the traffic is registered as A2P, it faces **lower filtering risk**; in other words, messages are far more likely to be delivered than if you were using unregistered P2P routes (Source: support.telnyx.com).

- **Two-Way Communication & Flexibility:** Unlike a one-way short code program, 10DLC numbers fully support two-way messaging by design (they behave like normal phone numbers). This means businesses can engage in interactive conversations with customers. From a technical standpoint, you can also use the same 10DLC number for voice calls (in many setups) and fax, since it's a real phone number, enabling an omnichannel contact point (e.g., call or text the same number). This flexibility is useful for continuity and branding.

- **Better Accountability and Trust:** The required registration and vetting process, while it adds overhead, ultimately improves the trust in the ecosystem. Carriers know who is sending the messages and for what purpose, so they can enforce rules more precisely. Reputable businesses benefit because their messages aren't unknowingly lumped in with spammers. The concept of the **Trust Score** adds a reputation layer – if you maintain good practices, you get higher throughput and less scrutiny over time. Essentially, 10DLC created a *more transparent and secure environment* for business texting (Source: campaignregistry.com), which in the long run benefits all legitimate senders and consumers (less spam).

- **Wide Range of Use Cases Supported:** With standard and special use cases defined, 10DLC can accommodate everything from tiny one-person businesses texting a handful of clients, up to large-scale notifications. The system's tiering (and exceptions like political and emergency classes) make it versatile. Carriers have shown willingness to adapt it to new needs (for instance, creating new special use categories as novel use cases arise), so it's a future-proof channel for most A2P needs.

Cons:

- **Registration Complexity and Delays:** The flip side of the compliance is the *hurdle it creates*. Businesses now must navigate a somewhat complex registration process (especially if they are not using a very user-friendly CSP). Providing accurate information, choosing the right

campaign type, and possibly waiting for vetting can be confusing and time-consuming, particularly for small businesses. If a campaign registration is rejected by a carrier, it may need revision and re-submission, causing delays in launching texting programs.

- **Additional Costs (Fees and Surcharges):** While cheaper than short codes, 10DLC introduced new fees that didn't exist for the old "uninhibited" long code messaging. Brands pay registration fees and monthly fees per campaign, which can add up if a company needs many campaigns (e.g., a large enterprise with multiple divisions might need separate campaigns). Moreover, carriers charge per-message fees on 10DLC traffic as a sort of "toll." For example, AT&T and T-Mobile charge around $0.003 per SMS on 10DLC, and Verizon about $0.0031 (Source: support.telnyx.com)(Source: support.telnyx.com). For large volumes, these surcharges are non-trivial. And if messages are sent without registration, the fees are even higher (AT&T unregistered traffic is $0.01 per SMS, T-Mobile $0.012 per SMS starting late 2024) (Source: support.telnyx.com)(Source: support.telnyx.com). So, businesses need to account for these in their budget, whereas previously they might have only considered basic SMS costs from their provider.

- **Throughput Limitations for Some:** Although 10DLC throughput is good, it's *managed*. If a business suddenly wants to send out an urgent blast beyond their allowed rate, they could be throttled. For example, an event notification system might find the daily cap on T-Mobile or the TPS limits on AT&T restrictive if they didn't vet for higher tiers. Short codes would have handled the burst seamlessly. So 10DLC is not always suitable for extremely time-sensitive, large-scale broadcasts (e.g., warning 1 million people of a critical event in minutes). Additionally, some types of campaigns (like mixed use or low-volume) intentionally have lower limits (Source: callhub.io)(Source: callhub.io). Businesses have to carefully choose and sometimes pay for vetting to get the limits they need.

- **Evolving Rules and Uncertainty:** The 10DLC ecosystem is still evolving, with carriers updating rules and fees relatively frequently. For instance, AT&T changed its fee structure in Oct 2024 to introduce new charges (Source: telgorithm.com), and T-Mobile has tweaked its policies (like waiving or instituting certain fees, changing vetting score interpretations, etc.). Verizon might introduce new measures in the future. This dynamic environment means businesses and CSPs must stay on top of changes to avoid service disruption or unexpected costs. There can be confusion about what is allowed; for example, content that might be fine on one carrier could be flagged on another if interpreted differently against their code of conduct. "Lack of transparency" has been a complaint, especially aimed at Verizon's unknown throughput calculation (Source: telnyx.com) and, early on, how exactly trust scores were determined. This can make it hard to plan campaigns with certainty.

- **Strict Enforcement and Penalties:** Mistakes or non-compliance can be costly. The carriers have set steep fines for violations (as discussed, e.g., $10,000 for certain spam/content violations on T-Mobile (Source: support.bandwidth.com)). If a business inadvertently violates these (say by texting people who didn't properly opt in, or by including prohibited content), they could face these pass-through fines. Also, if one's campaign gets suspended, it could interrupt critical communications. In short, the stakes are higher to "do it right," which is good for consumers but requires diligence by senders.

- **Not Global:** It's worth noting that 10DLC is a U.S.-centric solution. If a business has international audiences, 10DLC registration doesn't apply outside the U.S. Different countries have their own rules and number types. So 10DLC benefits only apply when messaging U.S. phone numbers. (Conversely, short codes have to be country-specific as well. Toll-free has some cross-country portability like Canada/U.S. for certain providers, but in general, each region has its system.)

In balancing these pros and cons, many businesses find that the **pros outweigh the cons** for their purposes – hence the rapid adoption of 10DLC since 2021. However, some also opt for a mix: for instance, use a short code for marketing blasts (to leverage high throughput and memorability) and use 10DLC numbers for more personalized interactions. The good news is that with compliance now standardized, whichever channel is used, the baseline of *permission-based, high-quality messaging* is enforced across the board.

Pricing Models and Carrier Throughput Expectations

Pricing for 10DLC messaging can be considered in two parts: **upfront/recurring costs** (registration fees, monthly fees) and **per-message costs** (carrier surcharges and SMS charges). Alongside pricing, understanding the throughput (rate limits) imposed by carriers is crucial for capacity planning. We've touched on throughput in an earlier section; here we consolidate the expected throughput and fees across major U.S. carriers:

1. 10DLC Registration Fees: These are fees payable to The Campaign Registry (often collected via your CSP). As of 2024, typical fees are:

- **Brand Registration:** $4 one-time for a Standard brand (for major businesses). If secondary vetting is requested, an additional fee (often $40) may apply; some CSPs bundle this (e.g., Twilio charges $44 which includes vetting). For Sole Proprietor brands, there's usually a separate registration path (often around $4 as well, but with extra identity verification steps).

- **Campaign Registration:** $10 one-time (this covers manual review by carriers via TCR) (Source: support.telnyx.com)(Source: support.telnyx.com). This fee is per campaign (use-case). If you later need to change the campaign details significantly, a new registration might be needed, incurring a new fee.
- **Monthly Campaign Fee:** Each active campaign incurs a monthly fee, roughly $2 for basic low-volume campaigns up to $10 for certain higher-volume or special campaigns (Source: support.telnyx.com). For example, a standard marketing or mixed campaign might be $10/month, whereas a strictly low-volume informational campaign might be $2/month. These fees often correspond to how the carriers classify the campaign's intensity.
- (Note: Non-profit or political campaigns sometimes have different fee structures; e.g., carriers often waive campaign fees for registered 501(c)(3) charity campaigns, and political campaign fees might be slightly different due to extra verification steps.)

2. Per-Message Carrier Surcharges (Registered Traffic): Each outbound message (and in some cases inbound) using 10DLC to US carriers will have a surcharge applied by that carrier. These fees are "pass-through" – meaning your messaging provider collects them to pay the carrier. Here is a **table of surcharges** for the major carriers for *registered* 10DLC traffic (as of late 2024):

CARRIER	SMS SURCHARGE (PER MESSAGE)	MMS SURCHARGE (PER MESSAGE)
AT&T	$0.003 *outbound* (inbound free) (Source: support.telnyx.com)	$0.0075 *outbound* (inbound free) (Source: support.telnyx.com)
T-Mobile	$0.003 *per message* (both outbound and inbound) (Source: support.telnyx.com)	$0.010 *per message* (both outbound and inbound) (Source: support.telnyx.com)
Verizon	$0.0031 *outbound* (inbound free) (Source: support.telnyx.com)	$0.0052 *outbound* (inbound free) (Source: support.telnyx.com)
US Cellular	$0.005 *outbound* (inbound free) (Source: support.telnyx.com)	$0.01 *outbound* (inbound free) (Source: support.telnyx.com)
Other carriers	Varies (generally similar small fees, or none)	Varies (MMS often $0.01 if applied)

Notes: T-Mobile uniquely charges for both sending and receiving messages on 10DLC. AT&T and Verizon currently do not charge for inbound messages (the business does not pay when a user replies). Also, these rates are for registered campaigns. **Unregistered 10DLC traffic**, if sent, carries *much higher* fees (and will soon be disallowed entirely). For example, an unregistered SMS sent to an AT&T user costs $0.01, and to a T-Mobile user $0.011–0.012 (Source: support.telnyx.com) (Source: support.telnyx.com) – several times higher than the registered rates, plus a high risk of blocking. The clear intent is to strongly discourage any unverified traffic.

Additionally, carriers have special fees for certain scenarios. T-Mobile, for instance, outlined fines for "spam" or "snowshoeing" (spreading traffic over many numbers to evade filters) – e.g., a $1,000 program evasion fee if caught (Source: support.bandwidth.com). T-Mobile also mentioned a fee for *Special Business Review* (SBR) requests ($5,000 for asking to exceed the 200k daily cap) (Source: support.bandwidth.com) and a fee for using custom alphanumeric sender IDs (which generally isn't applicable in the U.S. for A2P, so rarely encountered). In practice, most businesses will just see the standard surcharges above on their bills.

3. Throughput Expectations by Carrier: Summarizing earlier details, here's what to expect in terms of sending rates:

- **AT&T:** Throughput is determined per *Campaign* based on AT&T's internal "message class" assignment. For a well-vetted campaign in the standard use-case categories, you can get **up to 4,500 SMS per minute** (75 per second) for the highest tier (Source: redoxygen.com). Lower tiers might be 2,400/min (Source: redoxygen.com), 240/min, or as low as 75/min for an unvetted small sender (Source: redoxygen.com). MMS is typically counted separately but with similar scaling (e.g., 2400 MMS/min for top tier) (Source: support.telnyx.com)(Source: support.telnyx.com). AT&T's limits are applied per campaign (not per number, if you have multiple numbers on one campaign, it's shared across them).

- **T-Mobile:** Throughput is effectively capped by the **daily limit per Brand**. For a new unvetted brand, that's 2,000 messages/day to T-Mobile users (Source: support.bandwidth.com). With vetting, this increases to 10k, 40k, or 200k per day depending on trust score tier (Source: support.bandwidth.com). If you need to send to, say, 100k T-Mobile customers in a day, you *must* have a higher-tier trust or else you'll hit the cap halfway. In terms of instantaneous rate, T-Mobile doesn't publish a fixed TPS; anecdotal evidence suggests even high-volume brands might be practically limited to around 50 TPS towards T-Mobile. However, since the daily cap is the primary mechanism, one could theoretically send in a burst until the daily quota is exhausted (e.g., 200k in an hour, though that might trigger carrier scrutiny).

- **Verizon:** Expect high capacity – generally, Verizon allows traffic to flow up to the network's comfort. 6,000 messages per minute (100 per second) per 10DLC campaign has been cited as a guideline (Source: redoxygen.com). Many CSPs simply state that Verizon "will not be the bottleneck" if you are compliant. One thing to note is Verizon historically did not charge for 10DLC at first but later introduced the small surcharge above, showing they are onboard with the program but still somewhat hands-off in terms of micro-managing throughput tiers.

- **Other carriers:** Most other U.S. carriers have relatively small subscriber bases (so your traffic to them is a minor portion). They typically don't have special throttling beyond maybe a baseline like "30 TPS" each. The "Total MPS to minor carriers" in Twilio's docs (75 MPS for top tier) implies smaller carriers combined might allow up to that level (Source: callhub.io).

4. Messaging Provider (CSP) Considerations: It's important to mention that your messaging provider may also implement its own rate limiting or smart queueing. For example, some providers, like Telnyx and Telgorithm, highlight features like "automatic queueing to send at the exact carrier limit" (Source: telgorithm.com)(Source: telgorithm.com). This is to prevent messages from being rejected for going over the limit – instead they will queue and send when possible, which avoids wasted messages (since carriers still charge even for blocked messages in some cases). Providers might also spread traffic across multiple long code numbers if appropriate (though all must be registered campaigns). When you register campaigns via a provider, they often tell you your initial throughput assignment. If you need more, you can request vetting or submit a special request (and pay any associated fees).

5. Example of Cost & Throughput in Practice: Suppose a business registers one campaign for marketing with one 10DLC number. They pay $4 (Brand) + $10 (Campaign) upfront. They pay maybe $10/month for that campaign. If they send 100,000 texts in a month evenly across carriers: let's say 40% AT&T, 40% T-Mobile, 20% Verizon as a split. The surcharge cost would be: 40k * $0.003 (AT&T) + 40k * $0.003 (TMO) + 20k * $0.0031 (VZW) ≈ $300 in surcharges. The SMS delivery cost itself (what the CSP charges per SMS) is separate, but typically around $0.0025–$0.005 per SMS depending on volume, which would be another $300 or so. So total variable cost might be ~$600 for 100k messages, plus the fixed campaign fee. This is still far cheaper than doing 100k messages via a short code program if you factored in the monthly code lease cost. Throughput-wise, if that company had a medium trust score, they might have, for example, 2,400 TPM on AT&T and 10k/day on T-Mobile. If they try to send all 100k in one day, T-Mobile would be the choke point (max 10k delivered that day, remaining 30k to TMO users would spill to next days). They'd likely either spread out sends over multiple days or improve their trust score to raise the cap.

In planning any 10DLC campaign, understanding these throughput constraints per carrier is key to setting expectations on how fast messages can go out. Often, if high speed is needed across all carriers, obtaining a better trust score (via vetting) or even securing a short code for a parallel campaign might be considered.

Emerging Trends and Developments in the 10DLC Ecosystem

Since its inception, 10DLC A2P messaging continues to evolve. Industry stakeholders are actively refining the system as new needs and challenges emerge. Here are some of the notable recent trends and future developments to watch in the 10DLC space:

- **Stricter Enforcement and Deadlines:** Carriers have been gradually tightening the screws on unregistered messaging. Early on, there were grace periods where unregistered long-code messages were still delivered (albeit with higher fees and filtering). Now we are at the point where **unregistered 10DLC traffic is being outright blocked**. In fact, starting **February 2025, major carriers intend to block any A2P messages sent from long codes that are not registered** (Source: support.telnyx.com). This effectively finalizes the transition to 100% compliance on 10DLC. Businesses that have not yet registered their traffic have a hard deadline to do so or lose the ability to text customers. This also means the “whitelisting” exceptions or interim grey routes are closing. The ecosystem is moving to a fully closed-loop system where if it’s not in TCR, it won’t be delivered.

- **Fee Adjustments and Increases:** Carriers are revisiting their fee structures over time. For example, AT&T announced increased pass-through fees effective Oct 2024, including introducing a small charge for inbound toll-free messages and raising MMS fees (Source: telgorithm.com). T-Mobile likewise signaled that some previously waived fees (like the Grey Route fine or SBR fee) could be enforced in the future (Source: support.bandwidth.com) (Source: support.bandwidth.com). These changes indicate carriers are looking to balance revenue and cost as messaging volumes grow, and perhaps to further discourage undesirable traffic patterns by making them costly. We might see **annual or bi-annual fee reviews** by carriers, so businesses should stay alert to communications from their CSPs about any fee changes (usually given with some notice before taking effect). The trend is that A2P messaging will gradually become pricier on a per-message basis (though still low in absolute terms) – somewhat analogous to how telecom carriers treat commercial traffic differently from person-to-person texting included in user plans.

- **Improved Vetting and Scoring Mechanisms:** The concept of the Trust Score is also evolving. Initially, some businesses were surprised by low trust scores that limited their throughput, not fully understanding the criteria. TCR and vetting partners are working to improve transparency. We are likely to see more guidance on how to improve trust scores (for instance, by having a Dun & Bradstreet listing, good web presence, no prior spam flags, etc.). Also, the scoring algorithms might be refined to reduce false negatives (legitimate businesses getting low scores) and to maybe incorporate ongoing sending behavior (i.e., dynamic scoring). For special cases like political campaigns, the process via Campaign Verify remains in place (with an "Active" status instead of numeric score) (Source: callhub.io), but for standard brands the scoring could start to incorporate feedback. Some industry discussions even suggest that **message deliverability metrics** (how users engage or complain) might eventually loop back into a brand's reputation scoring. While not formally in place yet, the tools exist for carriers to monitor opt-out rates or complaint rates per campaign and theoretically downgrade a campaign's allowed throughput if it looks spammy. In short, 10DLC could become more *adaptive* in its control – rewarding good actors and penalizing bad actors in near-real-time.

- **Campaign Content and AI Monitoring:** As volumes increase, carriers are leveraging more advanced techniques (including AI-based content analysis) to monitor messages for compliance. There's an emerging trend of content rules being explicitly codified – for example, certain keywords automatically triggering scrutiny. One current example: SHAFT content (sex, hate, alcohol, firearms, tobacco) is disallowed for marketing, and if those keywords appear, it might trigger filtering unless the campaign is specifically entitled (e.g., a charity doing alcohol responsibility awareness might need special carrier clearance). We might see *automated compliance checking* at campaign registration – e.g., some CSP portals now warn you in real time if your sample content might violate rules. This is likely to improve, reducing the back-and-forth of campaign approval.

- **Interoperability and Wider Adoption:** While U.S. carriers are fully on board with 10DLC, the concept is now catching attention globally. Other countries, which may have traditionally had either strict short code regimes or no clear A2P distinction, are looking at similar models. We might see Canada adopt a parallel 10DLC registration system (currently Canada allows long code A2P with fewer restrictions, but spam growth may change that). Some aggregators are pre-emptively extending the idea of brand registration to other regions via initiatives like *Cloud Communications Alliance*. This means in the future, a global brand registry could exist where companies register once and have recognized identities in multiple countries' messaging networks. It's speculative, but 10DLC's success is a case study that might be exported.

- **Rich Messaging and 10DLC:** As messaging evolves beyond SMS into richer formats (MMS, and RCS – Rich Communication Services), the 10DLC framework could play a role in identity and trust for those channels too. RCS, often branded as "Chat" or "Business Chat" on Android, uses verified sender profiles and is currently separate from SMS short codes/long codes. But some industry voices suggest aligning these – for instance, using the same phone number for SMS and RCS channels for a business, and perhaps managing verification in a unified way. If RCS uptake grows (with features like branding, app-like interactions in messages), we may see The Campaign Registry or CTIA expand guidelines for those. Already, RCS business messaging has its own verification (with carriers and Google), but a unified registry could simplify trust across SMS and RCS. For now, this is an area to watch, as businesses might want consistent branding whether they message via SMS or RCS.

- **End-User Perception and Features:** Another trend is making messages more trustworthy and user-friendly. There's talk of carriers providing * indicators to users for verified business messages. For example, some carriers/apps may display a "verified sender" badge or the brand's name for text messages in the future (similar to how certain email clients show a verified logo for emails). This is not standard in SMS apps yet, but AT&T and T-Mobile have done trials with **registered sender display**, particularly in RCS but conceptually could come to SMS (maybe through app integrations). The groundwork of 10DLC – having an official record of the brand behind the number – is what would enable such features. So, 10DLC might soon mean not just compliance behind the scenes, but a visual indicator to consumers that a given text is from a legit registered business.

- **Changes in Use Case Offerings:** The carriers and TCR sometimes update the catalog of supported campaign types. For instance, if a new category of messaging becomes popular (say, telehealth notifications or food delivery updates), they might create a more specific campaign type for it, possibly with custom throughput or pricing. Recently, **"Conversational" campaigns** were introduced by some providers for low-volume two-way messaging that looks more like person-to-person chat but technically from a business (Source: support.telnyx.com). This is targeted at use cases like a salesperson texting one-on-one with a client – still A2P, but very low volume per number. Carriers might allow slightly different rules (maybe allowing such conversational traffic to not need huge vetting, but keeping volumes low). We can anticipate more nuance like this: tailoring rules for different messaging patterns.

- **Industry Collaboration and Transparency:** Finally, an important positive trend is the increased collaboration in the messaging industry on fighting spam. The 10DLC system is a product of that collaboration (between carriers, CTIA, TCR, and messaging providers). They continue to

share data (e.g., information on bad actors, spam trends). As this ecosystem matures, legitimate businesses will likely benefit from more consistent experiences across carriers – the goal is to remove the guesswork. The CTIA's 2023 updated guidelines are evidence of ongoing efforts to clarify expectations (Source: didforsale.com). We may see yearly (or as-needed) updates to these guidelines to address new issues (like robotext scams, etc.). The messaging community (via forums, conferences, etc.) is actively discussing things like having *standard metrics for compliance* or *appeal processes* if a campaign is mistakenly blocked. Greater transparency – for example, carriers providing reason codes when a message is blocked (e.g., "blocked due to SHAFT content") – is something businesses are asking for. If implemented, that would help companies quickly rectify issues and maintain good standing.

In conclusion, the 10DLC ecosystem, while now fairly established, is not static. It's moving toward a future of more **trusted, rich, and intelligent messaging**. Businesses adopting 10DLC should keep an eye on these developments. Staying compliant is an ongoing task, but with that comes the reward of reliably reaching customers on what remains one of the most effective communication channels: text messaging. The introduction of 10DLC has ushered in a new chapter where that effectiveness can be sustained without drowning in spam – a benefit to consumers and legitimate businesses alike, as the system continues to refine itself for the ever-growing demands of mobile communication.

Sources:

1. CTIA Messaging Principles and Best Practices (2023) (Source: 10dlc.org)
2. Telnyx – 10DLC FAQ and Compliance Guide (Source: support.telnyx.com)(Source: support.telnyx.com)
3. Charleston Telecom Solutions – *History of 10DLC Registration* (Source: charlestontelecomsolutions.com)(Source: charlestontelecomsolutions.com)
4. TJ Thinakaran's Blog – *Origins of 10DLC* (Industry Pilot Story) (Source: tjthinakaran.blog) (Source: tjthinakaran.blog)
5. TrueDialog – *Guide to 10DLC Registration & Regulations* (Source: truedialog.com)(Source: truedialog.com)
6. The Campaign Registry – Official Website (Source: campaignregistry.com)(Source: campaignregistry.com)

7. Telnyx – 10DLC Throughput Tables and Fees (Source: support.telnyx.com)(Source: support.telnyx.com) (Source: support.telnyx.com)
8. Bandwidth – T-Mobile 10DLC Guidelines (Source: support.bandwidth.com)(Source: support.bandwidth.com)
9. CallHub – 10DLC Trust Score Guide (Source: callhub.io)(Source: callhub.io)
10. Infobip – Comparing 10DLC, Short Codes, Toll-Free (Source: infobip.com)(Source: infobip.com)
11. T-Mobile Code of Conduct Highlights (via Bandwidth) (Source: support.bandwidth.com) (Source: support.bandwidth.com)
12. Telgorithm – Sole Proprietor Limits and 10DLC Fees Update (Source: telgorithm.com)(Source: telgorithm.com)

Tags: 10dlc, a2p messaging, sms, mms, business texting, long code, carrier regulations, telecommunications, messaging compliance, us messaging

---

About ClearlyIP

ClearlyIP Inc. — Company Profile (June 2025)

---

1. Who they are

ClearlyIP is a privately-held unified-communications (UC) vendor headquartered in Appleton, Wisconsin, with additional offices in Canada and a globally distributed workforce. Founded in 2019 by veteran FreePBX/Asterisk contributors, the firm follows a "build-and-buy" growth strategy, combining in-house R&D with targeted acquisitions (e.g., the 2023 purchase of Voneto's EPlatform UCaaS). Its mission is to "design and develop the world's most respected VoIP brand" by delivering secure, modern, cloud-first communications that reduce cost and boost collaboration, while its vision focuses on unlocking the full potential of open-source VoIP for organisations of every size. The leadership team collectively brings more than 300 years of telecom experience.

---

2. Product portfolio

- **Cloud Solutions** – Including *Clearly Cloud* (flagship UCaaS), **SIP Trunking**, **SendFax.to** cloud fax, **ClusterPBX OEM**, **Business Connect** managed cloud PBX, and **EPlatform** multitenant UCaaS. These provide fully hosted voice, video, chat and collaboration with 100+ features, per-seat licensing, geo-redundant PoPs, built-in call-recording and mobile/desktop apps.
- **On-Site Phone Systems** – Including CIP PBX appliances (FreePBX pre-installed), ClusterPBX Enterprise, and Business Connect (on-prem variant). These offer local survivability for compliance-sensitive sites; appliances start at 25 extensions and scale into HA clusters.
- **IP Phones & Softphones** – Including CIP SIP Desk-phone Series (CIP-25x/27x/28x), fully white-label branding kit, and *Clearly Anywhere* softphone (iOS, Android, desktop). Features zero-touch provisioning via Cloud Device Manager or FreePBX "Clearly Devices" module; Opus, HD-voice, BLF-rich colour LCDs.
- **VoIP Gateways** – Including Analog FXS/FXO models, VoIP Fail-Over Gateway, POTS Replacement (for copper sun-set), and 2-port T1/E1 digital gateway. These bridge legacy endpoints or PSTN circuits to SIP; fail-over models keep 911 active during WAN outages.
- **Emergency Alert Systems** – Including **CodeX** room-status dashboard, **Panic Button**, and **Silent Intercom**. This K-12-focused mass-notification suite integrates with CIP PBX or third-party FreePBX for Alyssa's-Law compliance.
- **Hospitality** – Including **ComXchange** PBX plus PMS integrations, hardware & software assurance plans. Replaces aging Mitel/NEC hotel PBXs; supports guest-room phones, 911 localisation, check-in/out APIs.
- **Device & System Management** – Including **Cloud Device Manager** and **Update Control (Mirror)**. Provides multi-vendor auto-provisioning, firmware management, and secure FreePBX mirror updates.
- **XCast Suite** – Including Hosted PBX, SIP trunking, carrier/call-centre solutions, SOHO plans, and XCL mobile app. Delivers value-oriented, high-volume VoIP from ClearlyIP's carrier network.

---

3. Services

- **Telecom Consulting & Custom Development** – FreePBX/Asterisk architecture reviews, mergers & acquisitions diligence, bespoke application builds and Tier-3 support.
- **Regulatory Compliance** – E911 planning plus **Kari's Law**, **Ray Baum's Act** and **Alyssa's Law** solutions; automated dispatchable location tagging.
- **STIR/SHAKEN Certificate Management** – Signing services for Originating Service Providers, helping customers combat robocalling and maintain full attestation.
- **Attestation Lookup Tool** – Free web utility to identify a telephone number's service-provider code and SHAKEN attestation rating.
- **FreePBX® Training** – Three-day administrator boot camps (remote or on-site) covering installation, security hardening and troubleshooting.

- **Partner & OEM Programs** – Wholesale SIP trunk bundles, white-label device programs, and ClusterPBX OEM licensing.

---

4. Executive management (June 2025)

- **CEO & Co-Founder: Tony Lewis** – Former CEO of Schmooze Com (FreePBX sponsor); drives vision, acquisitions and channel network.
- **CFO & Co-Founder: Luke Duquaine** – Ex-Sangoma software engineer; oversees finance, international operations and supply-chain.
- **CTO & Co-Founder: Bryan Walters** – Long-time Asterisk contributor; leads product security and cloud architecture.
- **Chief Revenue Officer: Preston McNair** – 25+ years in channel development at Sangoma & Hargray; owns sales, marketing and partner success.
- **Chief Hospitality Strategist: Doug Schwartz** – Former 360 Networks CEO; guides hotel vertical strategy and PMS integrations.
- **Chief Business Development Officer: Bob Webb** – 30+ years telco experience (Nsight/Cellcom); cultivates ILEC/CLEC alliances for Clearly Cloud.
- **Chief Product Officer: Corey McFadden** – Founder of Voneto; architect of EPlatform UCaaS, now shapes ClearlyIP product roadmap.
- **VP Support Services: Lorne Gaetz** (appointed Jul 2024) – Former Sangoma FreePBX lead; builds 24×7 global support organisation.
- **VP Channel Sales: Tracy Liu** (appointed Jun 2024) – Channel-program veteran; expands MSP/VAR ecosystem worldwide.

---

5. Differentiators

- **Open-Source DNA:** Deep roots in the FreePBX/Asterisk community allow rapid feature releases and robust interoperability.
- **White-Label Flexibility:** Brandable phones and ClusterPBX OEM let carriers and MSPs present a fully bespoke UCaaS stack.
- **End-to-End Stack:** From hardware endpoints to cloud, gateways and compliance services, ClearlyIP owns every layer, simplifying procurement and support.
- **Education & Safety Focus:** Panic Button, CodeX and e911 tool-sets position the firm strongly in K-12 and public-sector markets.

In summary

ClearlyIP delivers a comprehensive, modular UC ecosystem—cloud, on-prem and hybrid—backed by a management team with decades of open-source telephony pedigree. Its blend of carrier-grade infrastructure, white-label flexibility and vertical-specific solutions (hospitality, education, emergency-compliance) makes it a compelling option for ITSPs, MSPs and multi-site enterprises seeking modern, secure and cost-effective communications.

DISCLAIMER