Docs and FAQs

- So Your Calls are Being Marked as SPAM (But What If They’re Not?)
- What is a remote desktop?
- What is screen sharing?
- Shared Parking Vs. Park Orbit
- Which Client? PWA vs Desktop vs Native App
- Uninstalling the Desktop App
- Your step-by-step guide to 10DLC brand registration
- What is A2P messaging?
- What is 10DLC? Everything you need to know
- Compliance, user experience, and 10DLC campaigns
- Frequently asked questions about 10DLC
- SMS compliance guide and checklist
- Quick Guide to 10DLC - Everything you wanted to know!
- eFax Management - Report Access Changes

So Your Calls are Being Marked as SPAM (But What If They’re Not?)

Oh no! If your customers have stopped answering, it might be because they’re seeing calls from your phone numbers displayed as SPAM LIKELY or SPAM RISK via caller ID. Each phone carrier keeps a list of numbers they determine to be spam risks based on the history of the number, crowdsourced feedback and complaint data, and reputation analytics. Some of the most common reasons for getting a spam flag include:



1. The volume of outbound calls per day, per number, is high.
2. Someone flagged a call from your number in their carrier’s network database (perhaps before you even bought that new number).
3. The Outbound Caller ID number is not set properly in the invite and if invalid or incomplete, may be marked as spam automatically.

How Does This Happen–And Why Me?!

In response to the growing number of scam calls to mobile phones, many carriers and third parties have created tools to identify and block scam calls. Unfortunately, these tools aren’t perfect and they cast a wide net. Businesses may have their numbers incorrectly marked by scam ID technology, particularly when calling cell numbers. There are several technical triggers:

- Carrier spam features/apps that are automatically enabled on mobile devices. When someone calls one of these devices, the carrier checks the number against its database of reported scam numbers. If the source matches a reported scam number, the person being called sees a message that says “Scam Likely” alongside standard caller ID. The user can then decide whether or not to answer the call.
- In addition to “Scam ID,” carriers also allow customers to opt in to a “Scam Block” feature that prevents all Scam Likely calls from ever reaching the user’s phone in the first place. All of the carriers have now introduced their own paid and free versions of this service. Third-party apps also allow smartphone users to detect, report, and block scam calls.
- The Scam Likely Caller ID features will sometimes mark legitimate calls incorrectly, such that some people may report your number without even answering the phone. If this happens enough, your number will be marked Scam Likely.
- Carriers are also deploying algorithms in their networks to detect when a large number of phone calls originate from a common Caller ID number. They designate these calls as SPAM and display a “SPAM” message on the display of the receiving phone.

What to do? It’s critical that you’re able to call your customers and have them answer. Fortunately, there are ways to rectify the situation.

What’s the Fastest Way to Resolve It?

Unfortunately, there is no central database or service so far that manages this number flag, so it can sometimes take a little work to get it corrected. You can also take steps to avoid being flagged from the get-go.

Be Proactive

Encourage your customers to add your main number(s) to their contact lists, which supersede most carrier spam traps and allow calls to be delivered.

Next, register your numbers at the Free Caller Registry via https://www.freecallerregistry.com/fcr/. This helps register and whitelist your numbers with several top carriers and reduces the chances of them being flagged. The numbers and information provided will automatically be shared with all three of the Carrier Spam Monitoring Partners, namely HIYA, TNSI, and First Orion.

Getting your numbers registered has shown to be highly effective in protecting them from being flagged for many of the reasons listed above.

Get Your Number Removed from SPAM/SCAM Designations

Contact Carriers

You can use the links or email addresses below to register legitimate numbers and also address any incorrect labeling or call blocking with other carriers:

- **AT&T (HIYA)** https://hiyahelp.zendesk.com/hc/en-us/requests/new?ticket_form_id=824667
- **T-Mobile, Sprint (1st Orion)** https://calltransparency.com
- **Verizon, U.S. Cellular (TNS)** https://reportarobocall.com
- **Comcast, Charter, Cox, Altice and other fixed-line (VoIP) providers**
  Email Nomorobo for call blocking services: reports@nomorobo.com

Popular Spam Blocking Apps

In addition, here are some of the most popular spam blocking apps and contact info if you wish to reach out about being unflagged on their apps.

- **Robokiller –** Most popular call blocking app, millions of people have this application. Once you are blocked by them, every single user with the app will automatically have your number blocked. Email support@robokiller.com.
- **Nomorobo –** No Scoring/Rating System. Very Popular Call Blocking App. Winner of FTC Robocall Challenge. Email reports@nomorobo.com.

- **Icehook –** Will be marked as spam if it falls into “highly likely” / 81-100 risk level range. Contact them at https://www.icehook.com/contact
- **TrueSpam –** Uses a 0 – 100 Scale; flags occur with a score of 60+. Contact Info: https://www.truecnam.com/contact_us
- **Telo –** Nuisance score flagged at 65+, at which point they’ll notify you before your number is labeled a nuisance-level call at 70+. Contact https://www.telo.com

Third-Party Services

Last but not least, there are third-party services that can help get your numbers clean and keep them clean. For example, look into Caller ID Reputation Services like https://calleridreputation.com/ , or Numeracle’s Entity Identity Management platform, which prevents as well as remediates incorrect call blocking and labeling events

by Katie Reddick

What is a remote desktop?

A remote desktop is a program or operating system feature that enables your device to be remotely accessed or controlled by a user in a separate location from a separate PC or mobile device. Remote desktops can be used in sales, support and customer service functions to offer advice and guidance to clients. Remote desktop access functionalities include:

- Troubleshooting / Fixing Hardware Issues.
- Performing hands-on demonstrations.
- Installing and updating software.
- Accessing workplace computers whilst working remotely.

Why should I invest in remote desktop software?

Use the WebMeeting Remote Control client to connect to and control a computer remotely from anywhere around the world. The Remote Control client enables secure and reliable remote Windows desktop connections for both IT professionals and everyday users, to provide assistance, support, or demonstrate your products and services on remote PCs. Simply have the meeting participant install the WebMeeting Remote Control client on their machine and quickly start your remote control session within 5’.

Screen Sharing in a Web Meeting - Screenshot

Are remote desktops secure?

It's important to choose a remote desktop application from a trusted provider in order to guarantee that your data and other sensitive material remains protected. When choosing your remote application, make sure that remote sessions are encrypted and only accessible by authorised users. Never grant remote access permissions to a user who contacts you first. Where possible, only allow a trusted IT partner to conduct viewing sessions.

Would I need to install software on both devices?

Until fairly recently, to setup remote access you typically need to install and configure various software components and libraries on both machines; the controller and the one controlled BEFORE access could even be requested. This made troubleshooting on the behalf of clients cumbersome and time-consuming. However, with the introduction of Google's WebRTC protocol, things became a lot simpler! Using only a web browser and a secure video conferencing solution you can now initiate a remote desktop session in just a few clicks. All that's required is for the controlled PC to download a simple plugin before access can be enabled. Say goodbye to remote desktop clients and complex installs!

What remote control functionality does 3CX offer?

The video conference solution for business by 3CX has an inbuilt remote control feature that can be used to connect to and control a computer remotely from anywhere in the world. The Remote Control client offers secure and reliable remote Windows desktop connections for both IT professionals and everyday users. Use it to provide assistance, support, or demonstrate your products and services on remote PCs. Just fire-up 3CX WebMeeting and send a request to remotely control any of the invited participant's PCs. There's no specialist software required, just a quick to install plugin for the PC that's going to be controlled. Then, use WebMeeting’s file sharing feature to transfer, backup and restore mission-critical files.

Key features

- Initiate remote control through WebMeeting.
- Simple and quick installation.
- Compatible with Windows security framework and UAC (User Account Control).
- Record remote control sessions and share with participants.
- File transfer via built-in WebMeeting file sharing.
- Shared local-remote clipboard.
- GPU-acceleration for better performance.
- Low system resource usage.

What is screen sharing?

Screen Sharing or desktop sharing technology enables you to share your entire screen or a specific window with other computers. Using specialist technology or plugins, presenters can give remote users permission to view on-screen activity from their own device. Screen sharing is sometimes confused with 'Team Viewing' or remote desktop capabilities. Whilst all three techniques allow a remote device to view a computer screen, screen sharing technology does NOT grant permission to control or make changes to the viewed computer. For this reason, screen sharing is primarily used as a collaboration and presentation tool. In this capacity, it can dramatically improve your sales, support and customer service!

Screen Sharing

What are the applications of screen sharing?

Perfect pitches and meetings

Executing the perfect sales pitch over the phone can be tough, but it doesn’t need to be. Desktop sharing makes it possible to show remote attendees everything your business offers without even leaving the office. Take prospects virtually by the hand and guide them through your product or service offerings. Whether you need to carry out meetings or present pitch decks and sales presentations, you will save time and expense by conducting them remotely using screen sharing in conjunction with your video conferencing solution.

Train customers and staff effectively

Easily roll out new products and services across your business sharing your desktop with multiple meeting participants. The physical limits of the office are no longer a barrier as you use screen sharing to collaborate with team members in real-time, regardless of where they are located in the world! By sharing the same screen content, such as an image, a graph, or a chart, your participants can see exactly what you are referring to avoiding any confusion or misunderstanding.

Boost your customer service

Screen share can also be used in a customer service or support capacity. Troubleshoot customer and colleagues queries, regardless of the distance between you! Your employees can be in any location and can still collaborate and learn from fellow team members. Additionally, customers who need assistance with new software, working through technical problems, or changing settings can use a screen sharing feature to have a 1-1 conversation with a technical advisor who can walk them through step by step.

What are the benefits of screen sharing?

Using a screen sharing feature saves time and money. Rather than having to travel to your client's site each time you want to discuss a new sales opportunity or offer training, you can conduct the session remotely without needing to worry that key information will get lost in translation. By incorporating sharing alongside your video conferencing solution, you'll reduce local travel and the need for oversea's business trips- just imagine the financial and environmental benefits! Invite your customers to a web meeting, begin sharing your screen and interact with them as if you were face to face.

What does 3CX offer?

3CX's integrated secure video conferencing software transforms two-dimensional audio communication into an interactive, audiovisual experience that makes meetings more productive. Simply launch or schedule your WebMeeting session, invite the desired participants and click the screen share icon to get started! You can even screen-share with video and audio playback to add some flair to your presentations! There's no need to purchase any additional software or install a plugin, all that's required is an active internet connection and a google chrome or safari web browser.

Key features:

- Share your desktop and other applications
- Easy to use
- Share documents and files
- Text chat and file transfer
- Whiteboard feature
- Screenshare with Audio

Shared Parking Vs. Park Orbit

A question 3CX support often gets asked is, “What is the difference between shared parking and the park orbit?”. Overall, there are no differences in regards to what they both offer. Both are “slots” in which calls can be placed and retrieved. However, behind the scenes there are some vast distinctions between the two. Let’s untangle the cord.

Parking Orbits

Imagine parking orbits as “rooms” within 3CX. Calls can be placed into these “rooms” by transferring them from your IP phone or 3CX client. There are 10 rooms available and shared, unrestricted, between all users. A max. total of 64 calls can be placed into those rooms. Wait, 64 calls in 10 rooms? How does this work?

Get in

To park a call into a room press the transfer button on your SIP device followed by entering the number *0[0-9] (eg *00). The active call on your extension will be placed into room 0. The transferred party will be placed on hold.

It is possible to keep transferring more calls into *00, from your extensions or others, or to *01 even if there are calls in the room already. Don’t worry, calls held in a room cannot talk to each other, otherwise you would be in a conference call.

Get Out

To unpark a call which is parked in a room, create a new call from your SIP device to *1[0-9] (eg *10).

It is important to know that each and every extension in 3CX can unpark calls which have been parked by someone else. If the CEO parks an important business partner into a room, this call can be resumed by every other user of the system.

In the case that in a single room multiple calls have been parked, the call that was parked first will be retrieved first while using the matching dial code of the room (*10 for room 0). In case you need to selectively unpark a person from a room with multiple calls in it, you must use the 3CX client for Windows or Mac or the Web Client to do so.

Use Case I

I get a call from person A who needs to urgently talk to a colleague of mine. After an attempted transfer, I failed to get the requested colleague on the line. I decide to physically go and find the colleague in question. While I get up to go find the colleague, I place the caller into *00 and hang up my phone. Once I find the person I am looking for, who often happens not to be in their office, any SIP phone close to him/us will do the job. I dial *10 and hand over the call to my colleague. The result? A happy customer…

Use Case II

I have a SIP forked ID (meaning I have more than one SIP device on my extension) with a DECT phone and my 3CX client. I take a call on my 3CX client but I need leave my desk whilst on the call. So how do I transfer the call from me to myself? I transfer the call to *05 and then dial *15 on my DECT phone and I am good to go.

Shared Parking

Compared to the open parking space above, in shared parking the call flow is much more controlled. Firstly, there are 250 rooms and they are called SP[0-250].

These rooms can be provisioned onto a SIP device (3CX client and IP phone) which will give visual feedback about the state of the room (free or busy) on the respective BLF key. By simply pressing on the matching BLF key a call can be placed into a room and all extensions monitoring the same room on their SIP device will see that there is a call up for grabs.

There is also a limit of 1 person per room. Shared parking is a sort of replication of “shared line appearance” which you may be familiar with. Additionally, if you use the park function from the 3CX client or Web Client those calls will be placed into shared parking slots in an ascending free order.

Shared Parking Orbit of calls

Use Case

Assume that the reception has been tasked to distribute calls to the internal staff. For each member of staff a dedicated shared parking slot was allocated and provisioned onto their SIP device. On incoming calls the reception can monitor whether or not the requested person is available via the 3CX Switchboard. If not, instead of “terminating” the call, the call can be placed in the SP slot of the person. Once the person finishes their current call, the BLF on the person's SIP device indicates the next call to process which can be taken via a simple press of the BLF button.

Which Client? PWA vs Desktop vs Native App

Web client with BLF

The PWA (Progressive Web App) app

What is a PWA app?

PWA stands for Progressive Web Apps (PWAs). These are applications built using web technologies that can be installed and run on all devices from one codebase - in this case, our Web Client - which is also the basis for our Desktop App. A PWA provides native-like experiences and adapts to the capabilities supported by each device. Some characteristics:

- Works on Chrome and Microsoft Edge Chromium.
- Runs securely within the browser in its security framework and libraries.
- Zero admin - automatically updates.
- No local installation needed - no install or uninstall.
- Runs in the background and supports Push Notifications.

What does the 3CX PWA app do

- Fully functional 3CX client that feels/looks like a native app.
- Starts automatically upon starting the browser.
- Notifies user of incoming calls via a PUSH notification message box.
  - No need to be logged in to 3CX or even have the tab open.
  - In case of Edge, browser will be started if not active.
  - In the case of Chrome browser must be running.
- Launch calls in CRM or websites via Click2Call extension.
- Calls can be auto answered.
- Supports SSO.
- Fully supports Yealink, Jabra and soon Plantronics headsets.

- PWA works great on Microsoft Terminal Server - Read how to mass deploy.
- To be added in update 7a: Dialer will include the BLF panel.
- To be added in update 8: Be launched via the tel: protocol by 3rd party external apps.

PWA - Must haves \ Must dos

- PWA will only work for installations that have a fully qualified domain and a valid SSL certificate.
  - If you host 3CX in the cloud using a 3CX certificate, this is automatic.
  - If you have an on-premise installation, you must have configured Split DNS with a valid 3CX certificate or custom certificate. You are gonna need this anyway, sooner or later!
- You must set Google or Edge to auto start upon login to the OS. Here's how.

What PWA can not do

- Capture focus on incoming calls - Unfortunately, we have not found a way around this.
- Microsoft Tapi Integration for some older CRM/Accounting applications such as Datev.
- Launch External Applications upon receiving a call.

Desktop App

What is the Desktop App (also referred to as the Electron app)? The desktop app is a repackaged web client using the Electron framework. It allows control of the browser version of the browser as well as access to operating system functions.

It was this app that got compromised in the 3CX supply chain attack. This had nothing to do with the Electron framework or indeed any of the components we shipped in the Desktop app. The Desktop App was compromised because our network had been attacked by a hacker group. Our investigator Mandiant assesses with high confidence that UNC4736 has a North Korean nexus.

Read more about this here.

The compromised Desktop App has since been completely checked and cleaned and can be considered secure. We have put controls and procedures as well as tools in place to ensure supply chain attacks will not hit us again.

What the Desktop App can do in addition to the PWA

- Capture focus on incoming calls.
- Launch External Applications upon receiving a call.
- Dial or transfer using hotkeys.
- Allow for the dialer dialog to be moved around the screen separately from the main screen.

What the Desktop App can not do

- TAPI - ability to be launched by TAPI capable apps.
- If you close the app, then you will not be notified of incoming calls.

What the Desktop App requires

- Network wide antivirus and controls in case of emergency

Native App

3CX has native apps for all major operating systems - iOS, Android and Windows. These apps use SIP rather than WebRTC for calls. They operate entirely separate from the PBX using SIP authentication IDs rather than web authentication. This means that the maximum a hacker can do if it obtains access to these credentials is make and receive calls.

Whilst the iOS and Android apps are distributed via their app stores, the Windows app is distributed via the PBX. Currently, the native Windows app is also referred to as our Legacy app. This app works well and is secure, but has not been updated in a while. During the supply chain attack, this was a godsend. However, its architecture is out of date and needs to be redone.

We're now considering developing a new native Windows app that will look and behave like the iOS and Android apps. It would be distributed via the Microsoft store. This makes it inherently secure not only because the store checks the security of the apps before uploading, but also because in case of a security event, it allows for a much faster and automatic response.

What the Native App can do in addition to Desktop or PWA app

- Capture focus on incoming calls.
- Launch External Applications upon receiving a call.
- TAPI - ability to be launched or be launched from TAPI capable apps.

What the Native App requires

- Local admin rights to install the app.
- Provisioning via PNP on local LAN OR download of config file (U8).

Uninstalling the Desktop App

The Desktop App can be uninstalled as explained below. On some Windows machines where antivirus software already deleted some of the files the uninstaller may fail.

On Windows:

1. Start
2. Type “Control Panel”, Enter
3. Select “Programs and Features”
4. Find 3CX Desktop App, select and press “Uninstall”.

On Mac:

1. Go to “Applications”
2. Tap on “3CX Desktop APP”
3. Right click then “Move to Bin”
4. Ensure that it isn’t also present on Desktop otherwise delete it from there as well.
5. Empty the Bin

Mass / Network Uninstall of Electron App

Partners on our forums have kindly contributed Powershell scripts that allow companies to mass uninstall the electron app from their Network. We have merged them into one that will attempt to uninstall and forcibly delete any remaining files and entries associated with the Desktop App. We hereby thank the original authors of the scripts that were merged. This powershell script hasn't been thoroughly tested yet from our end, we recommend testing it on one machine first before executing it on your customers infrastructure. This must be run on client machines not the server.

Important: There are many scripts being suggested on the internet. Please be careful with any script or executable found on the internet, do not blindly trust them as they may be harmful.

```
# Kill 3CX processes first
Get-process | Where-Object {$_.name -Like "*3CX*"} | stop-process

# Attempt #1 - via EXE uninstall method
$3cxapps = Get-WMIObject -Class Win32_product | where {$_.name -like "3CX Desktop APP"}
foreach ($app in $3cxapps) {
```

```
try {
$app.Uninstall()
Remove-Item C:\Users\$env:UserName\AppData\Roaming\3CXDesktopApp -Recurse
Remove-Item C:\Users\$env:UserName\AppData\Local\Programs\3CXDesktopApp -Recurse
Remove-Item C:\Users\$env:UserName\Desktop\3CX Desktop App.lnk -Recurse
Write-Host "Uninstalled $($app.Name)"
}
catch {
Write-Host "Error uninstalling $($app.Name): $($_.Exception.Message)"
}
}

# Attempt #2 - via MSIEXEC ~ Requires Set-ExecutionPolicy to be changed
$appInstalled = Get-WmiObject -Class Win32_Product | Where-Object {$_.Name -eq "3CX Desktop App" }
if ($appInstalled) {
try {
$uninstallString = $appInstalled.UninstallString
Start-Process msiexec.exe -ArgumentList "/x `"$uninstallString`" /qn" -Wait -NoNewWindow
Remove-Item C:\Users\$env:UserName\AppData\Roaming\3CXDesktopApp -Recurse
Remove-Item C:\Users\$env:UserName\AppData\Local\Programs\3CXDesktopApp -Recurse
Remove-Item C:\Users\$env:UserName\Desktop\3CX Desktop App.lnk -Recurse
Write-Host "Uninstalled $($appName)"
}
catch {
Write-Host "Error uninstalling $($appName): $($_.Exception.Message)"
}
}
else {
Write-Host "$appName is not installed"
}
```

Your step-by-step guide to 10DLC brand registration

Today’s consumers expect instant communication, meaning businesses must constantly seek innovative ways to engage with their audiences. 10DLC is a powerful yet underutilized tool reshaping the landscape of application-to-person (A2P) messaging in the US. But why should businesses and marketers pay attention to 10DLC?

Understanding and correctly using 10DLC can significantly impact your business's communication strategy. It offers your audience a direct and personalized channel while helping you navigate the complexities of regulations and carrier guidelines. Use our six-step guide to register your brand with any carrier, and learn answers to common 10DLC questions.

What is 10DLC?

10DLC (10-digit long code) numbers let businesses send A2P text messages directly to individuals using a local number. Carriers have implemented this system to ensure businesses can reach out to customers in a trusted and regulated way, avoiding the pitfalls of spam and ensuring messages are welcome.

Essentially, the 10DLC classification focuses on making your business communications feel as personal and direct as chatting with a friend while ensuring your business stays compliant with best practices. Virtually all SMS and MMS sent by a business—even if manually triggered by a human—is considered A2P and, therefore, must be sent using 10DLC.

What is 10DLC brand registration, and why is it important?

10DLC brand registration is when you officially link your messaging campaigns to a recognized and approved 10DLC number. As we noted above, carriers require you to register your brand for any A2P messaging. Successfully completing the registration is like getting a badge of authenticity that tells the world you're the real deal.

Registering your brand for 10DLC lays the foundation for successful, respectful communication with your audience. It allows you to leverage the power of SMS marketing effectively and responsibly,

ensuring your messages are recognized and delivered.

Key benefits of 10DLC brand registration

Successfully completing 10DLC brand registration is your gateway to accessing several strategic advantages:

Enhanced deliverability

When carriers and networks recognize your numbers as registered and above board, it's like giving them a straight shot at your audience's inboxes. This boost in deliverability is thanks to the trust carriers have in brands that take the time to register. It means your messages are far more likely to be seen, read, and acted upon because they won’t get caught in spam filters.

Increased trust

Think of registration as your brand's promise to the world that you're all about honesty and integrity. It's a powerful statement that amplifies customers’ confidence in your brand, leads to deeper customer relationships, and lifts your brand's reputation.

Assurance of compliance

With ever-changing regulations and guidelines, 10DLC brand registration offers peace of mind that your SMS marketing efforts are compliant, minimizing the risk of penalties or disruptions. This assurance lets you focus on crafting impactful messages, knowing your operations align with industry standards.

The following section will guide you through the necessary steps to ensure your business is fully prepared and compliant for effective SMS marketing with 10DLC. This step-by-step approach will simplify the registration process, making it accessible and straightforward for businesses of all sizes.

6 steps for successful 10DLC brand registration

Starting your 10DLC brand registration journey is a strategic move toward optimizing your business messaging campaigns. Here’s a straightforward, six-step guide to help you navigate the process

with ease:

1. Determine your business type

Brands can choose between a few business types for registration:

- Private enterprise
- Government
- Publicly traded company
- Nonprofit
- Sole Proprietor

The designation you choose during this step will shape the rest of the registration process and what's required from you.

2. Gather essential information

You'll need the following information to register your brand:

- Your company's legal name
- The country where your business is registered
- What kind of organization you are
- Your Tax ID or EIN
- Your business website
- Descriptions and sample messages for each messaging use case

In addition to gathering the basic information listed, it's critical to also compile any specific documentation related to your organization type.

For instance, if you're registering as a nonprofit, be prepared to provide your 501(c)(3) certification. For private enterprises, relevant business licenses or incorporation documents might be necessary.

Collecting this information upfront will streamline the process, minimizing delays and potential complications.

3. Choose a registration platform

You'll want a platform that's supportive, easy to use, and flexible enough to adapt to your needs. Think about its reputation, the support it offers, how easily you can manage your campaigns, and its success rate with 10DLC registrations and staying compliant. The right platform will guide you through the registration process, offering insights and tools to make your messaging strategy shine. Vox Tandem is here to help!

4. Submit brand and campaign details

Now it's time to present your information via the registration platform. Detail your brand and outline each campaign you're eager to launch. Accuracy is key here. Make sure everything is consistent and correct across all documents and platforms to avoid any hiccups or delays in getting your registration approved.

5. Await approval

Approval times can be as varied as the weather, depending heavily on the carrier or provider, the complexity of your campaign, and how well you've filled out your application. The approval process can take anywhere from a few hours to several days.

Some providers, like Vox Tandem — known for its streamlined processes and direct connections — might get you through this step more quickly, sometimes within 24 to 48 hours.

6. Assign phone numbers

Once you've got the thumbs up, it's time to assign 10DLC numbers to your campaigns and kickstart your messaging. Choose your numbers, link each one to a specific campaign, set up your message flow, and then test and monitor everything to ensure it's running smoothly.

Common questions about 10DLC brand registration

Navigating the 10DLC brand registration process can be tricky. This section answers some of the most common questions we receive on 10DLC brand registration so you can move forward with confidence.

How often should I renew my 10DLC brand registration?

10DLC brand registration does not require frequent renewals in the traditional sense. Once your brand is registered and approved for 10DLC messaging, there’s no expiration as long as your use case and messaging practices remain consistent with the information you provided during registration.

However, it's important to keep your registration information up to date. If your business undergoes significant changes—think new messaging strategies, a spike in message volume, or even a brand makeover—it's time to refresh your registration to keep everything in sync.

And because regulations and carrier rules are always changing, staying in the loop with the latest requirements ensures your 10DLC efforts stay compliant.

What happens if I don't register my campaign?

If you don’t register your campaign, you may encounter reduced message deliverability, as carriers and service providers might block your messages. Unregistered campaigns are often flagged for non-compliance with messaging standards and regulations.

Plus, operating an unregistered campaign exposes you to the risk of incurring fines and penalties for non-compliance—for example, if you use gray routes or fail to follow the guidelines set by the CTIA.

Here’s everything Vox Tandem customers should know about the upcoming changes and how to prepare:

- What is 10DLC? Everything you need to know
- Unregistered 10DLC is ending: What you need to know
- Your step-by-step guide to 10DLC brand registration
- SMS compliance guide and checklist
- What is A2P messaging?

- Compliance, user experience, and 10DLC campaigns
- Frequently asked questions about 10DLC

Contact our team of experts to start the 10DLC approval process and start reaching more customers.

What is A2P messaging?

A2P (application-to-person) messaging is a type of SMS text messaging used to send messages from an application or software program to a mobile device or phone. As this method of communication is largely used by companies and organizations to communicate with customers and subscribers, A2P messaging is also often referred to as business SMS. Consumers will typically encounter A2P messages in the form of appointment reminders, order status updates or promotional messages.

How is A2P messaging different from P2P messaging?

The main difference between P2P (person-to-person) and A2P messaging is the origin of the messages in question. While a P2P message is sent from one person to another, an A2P SMS is an automated text sent via a messaging platform (application) to the recipient. But here's the twist:

"All messages sent from a business—even if they're sent by an individual and not an automated system—are considered A2P messages."

P2P VS A2P MESSAGING

As such, organizations must ensure that their messages comply with the Telephone Consumer Protection Act (TCPA). The TCPA protects consumers from unwanted or unsolicited communication from businesses. There are multiple guidelines laid out by TCPA, but to summarize, organizations should:

- Get written consent from consumers before beginning communications.
- Provide clear ways for consumers to opt in or out of messages.
- Include the organization's name in each message.
- Respect opt-outs and the Do Not Call Registry.

Check out our SMS compliance guide and checklist for more information on text messaging regulations.

What number types can you use with A2P messaging?

A2P messaging supports a range of number types depending on the messaging platform and the country where the numbers are used. In general, the most common number types used for A2P messaging include:

- **Short codes** are typically four- or five-digit numbers used for sending and receiving text messages. They're often used for marketing campaigns, voting, or other interactive messaging services.
- **Long codes** are regular phone numbers that can be used for A2P messaging. They're often used by businesses for two-way messaging, such as customer support and order tracking.
- **10DLC numbers** are 10-digit phone numbers specifically designed for A2P messaging. They are vetted by carriers to ensure compliance with industry standards and best practices, and they offer higher messaging throughput than long code numbers. Carrier vetting means messages sent from 10DLC numbers are more likely to be delivered quickly and reliably. In addition, 10DLC numbers offer more advanced messaging features, such as message templates, which can help businesses ensure compliance with carrier requirements and industry regulations.
- **Toll-free numbers** start with specific codes, such as 800, 888, or 877. They're often used for customer support, marketing campaigns, and other A2P messaging services.
- **Virtual phone numbers** aren't tied to a specific physical phone line. They're often used for A2P messaging in countries where short codes and long codes are not available.
- **Sender IDs** are alphanumeric strings that identify the sender of a message. Like virtual numbers, they're often used for A2P messaging services in countries where short codes and long codes are not available.

What are some A2P messaging use cases?

According to a recent report from Beyond Market Insights, the A2P SMS market is expected to grow from 62.2 billion in 2021 to 89.2 billion in 2030. That growth is largely due to the saturation of other channels such as email or social media and the relative cost-effectiveness of SMS communication.

Below are a few of the main ways your organization could leverage A2P messaging to communicate with customers, subscribers or prospects.

Multi-factor authentication (MFA)

MFA or two-factor authentication (2FA) are security methods used by many organizations to verify identities and prevent fraud. A 2FA message typically includes a one-time pin, code or link sent to a recipient’s phone to verify their account or a login attempt.

In industries with strict security regulations, such as finance or healthcare, MFA or 2FA technology is often required to access certain accounts or information.

Important alerts and updates

Organizations can also send an automated SMS to update customers about the status of their order or remind them of an upcoming appointment or reservation. These types of messages typically include a package tracking number, a link to an original order or a request to confirm an appointment time.

Even government entities use SMS to communicate with people. In the U.S., the Emergency Alert System (EAS) allows the President to alert Americans to national emergencies.

Marketing messages

On average, people receive around 100 emails per day - and nearly half of them are spam. To reach customers through a more personal, less saturated channel, more organizations are turning to SMS to conduct marketing campaigns and provide better customer service.

Compared to email, SMS also has a higher click-through rate (CTR). While nearly 20% of people will click a link sent in a text message, not even 4% of people will click a link received in an email.

Make sure your important messages reach their destinations

A2P messaging seems simple—find a messaging platform or set up a business phone and start texting your customers. However, the reality is more complex.

Compliance is the biggest reason that businesses need to choose a trusted provider for their A2P messaging. TCPA violators can be fined $500–$1,500 per non-compliant text. That’s a hefty fee for even one rogue SMS. But if you’re a business sending thousands of messages per day, you could be looking at a million-dollar fine.

And if you're investing in SMS communications to send important messages like appointment reminders or 2FA codes, you'll want to make sure that you're sending them over a reliable network. Sending undelivered texts into the theoretical void doesn't do your business—or your customers—any good.

Here's everything Vox Tandem customers should know about the upcoming changes and how to prepare:

- What is 10DLC? Everything you need to know
- Unregistered 10DLC is ending: What you need to know
- Your step-by-step guide to 10DLC brand registration
- SMS compliance guide and checklist
- What is A2P messaging?
- Compliance, user experience, and 10DLC campaigns
- Frequently asked questions about 10DLC

Contact our team of experts to start the 10DLC approval process and start reaching more customers.

What is 10DLC? Everything you need to know

In business communication, SMS and MMS messaging have proven to be powerful tools to reach customers directly. But how do you ensure your messages are delivered efficiently and compliantly?

A2P (application-to-person) texting allows businesses to communicate en masse without the tediousness of manual texting. But as the demand for A2P grows, so does the need for more efficient, compliant, and cost-effective solutions.

That's where 10DLC comes into play. 10DLC is the evolution of A2P messaging created in direct response to the industry's call for those efficient, compliant, and cost-effective solutions. Adopting 10DLC means you're aligning with a framework designed to optimize A2P messaging. The result? Enhanced reach, higher delivery rates, better compliance, and cost savings.

Recognizing the importance of 10DLC is essential for anyone involved in business messaging. In this blog post, we'll highlight its pivotal role in the A2P communication landscape and how it directly shapes the effectiveness and compliance of your messaging strategies. Stay informed and ahead of the curve by understanding the nuances of 10DLC.

What is 10DLC?

10DLC (10-digit long code) numbers are local long code numbers that mobile network operators approve for A2P messaging. This approval comes about by registering the local long code number with a verified 10DLC brand and campaign.

A 10DLC-registered long code number can support moderately large volumes of text messages. Carriers in the U.S. are implementing requirements that all A2P messaging uses 10DLC-registered numbers on their networks.

To fully understand 10DLC and its benefits, let’s take a look at how business text messaging has evolved over the years.

Evolution of business messaging

Until the late 2010s, many phone number types weren’t specifically designed to send mass SMS messages, which presented challenges like:

- Limited reach
- Potential compliance issues
- Inefficiencies in communication.

In subsequent years, telecom providers and regulatory bodies addressed these challenges by collaborating to introduce phone numbers optimized for bulk messaging.

Currently, the most common and cost-effective way for businesses to send SMS and MMS messages to customers is A2P (application-to-person) texting. A2P removes the manual labor of texting and enables businesses to send text messages in bulk.

Most American organizations can send messages from three types of numbers:

1. Toll-free long codes

Toll-free numbers are an affordable option for two-way SMS in moderately large volumes. Toll-free long code numbers can send and receive thousands of messages per day at high throughput rates. They’re also great for branding. Businesses can use number search tools to find branded vanity toll-free numbers (such as 1-866-FASHION).

Toll-free long code numbers require registration, and some carriers make the registration process complex and lengthy. Be sure to choose a carrier that makes registering and verifying your numbers simple. It's also worth noting that toll-free numbers can sometimes resemble international (non-US) numbers to your customers, limiting your campaign's engagement.

2. Short codes

Short code numbers are ideal for ultra-high volume traffic, like large-scale marketing campaigns from a custom recognizable number. While they boast impressive throughput, they come with a hefty price tag for setup and maintenance.

Additionally, their inability to handle phone calls can be a limitation for businesses seeking multi-channel communication. Despite supporting two-way messaging, the costs and restrictions often make businesses seek alternatives.

3. 10DLC numbers

While short codes are tailored for ultra-high volume traffic, they’re also burdened with significant setup costs and an inability to handle phone calls. And local long code phone numbers—primarily designed for person-to-person (P2P) texting—are limited in their messaging volume. Using them for

A2P messaging can also breach CTIA guidelines, leading to compliance concerns.

10DLC was created to bridge those gaps. It addresses the volume and compliance challenges of local long codes and sidesteps short codes' high costs and limitations. With 10DLC, businesses can harness the strengths of both channels without their inherent drawbacks, positioning 10DLC as the optimal choice for contemporary A2P messaging.

Benefits of 10DLC

10DLC numbers offer businesses a powerful combination: the ability to send mass text messages efficiently while keeping overhead costs low. Here's what sets 10DLC apart:

Higher SMS message volumes and increased throughput

10DLC numbers can send SMS message volumes that bridge the gap between the limits of short codes and toll-free long codes. This increased throughput ensures your messages are sent swiftly, reaching your audience when it matters most.

For a deeper dive into 10DLC use cases and throughput rules, see our 10DLC knowledge base.

Lower costs with added flexibility

10DLC numbers come with a more affordable price tag than other number types, which makes them an ideal choice for businesses that either can't justify the cost of a short code or simply don't need one. What's more, businesses can convert their existing landlines to 10DLC numbers, allowing them to send more messages without incurring the cost of an additional number.

Better deliverability and compliance

10DLC numbers have the advantage of being pre-approved by mobile network operators. Pre-approval ensures higher delivery rates and better compliance with carrier regulations, ensuring your messages reach their intended recipients without any hitches.

Who should consider using 10DLC?

10DLC isn’t a one-size-fits-all solution, but it caters to a wide range of businesses with specific needs.

Companies that want to balance volume and cost

If your business sends out a volume of messages that falls between the capacity of short codes and toll-free long codes, 10DLC is an ideal choice. It offers the flexibility of higher throughput without the high costs associated with short codes. To help you navigate the landscape of messaging options, check out this comprehensive guide to different number types and their throughput capacities.

Enterprises that need cost-effective messaging

For businesses that find short codes too expensive but need more capability than a regular long code, 10DLC offers a cost-effective alternative. 10DLC’s monthly costs are lower than dedicated short codes, making it an affordable choice for many.

Organizations that want to ensure compliance

With increasing regulations around messaging, businesses need to ensure they're compliant to avoid penalties. Since 10DLC numbers are pre-approved by mobile network operators, they reduce their risk of non-compliance.

Brands seeking better delivery rates

For businesses that have consistently encountered message deliverability barriers, 10DLC offers a distinct advantage. Its pre-approved status by mobile network operators eliminates the common delivery hurdles faced with other messaging formats. Skipping those hurdles means fewer undelivered messages, reduced chances of being flagged as spam, and a higher likelihood that your communications will land directly in the recipient's inbox, making 10DLC a transformative solution for business messaging.

Businesses looking for flexibility

10DLC provides a seamless transition for businesses looking to convert existing landlines to a format suitable for bulk messaging. So you can maintain your existing number while benefiting from the capabilities of 10DLC.

If your business experiences fluctuating messaging volumes, 10DLC also offers the flexibility to scale up or down based on your needs without incurring prohibitive costs.

When it comes to balancing cost, volume, deliverability, and compliance, 10DLC stands out as a top contender. However, it's crucial to evaluate your specific needs, messaging volume, and budget to determine if 10DLC is the right fit for you.

Get started with 10DLC

In today's world, where billions of SMS messages are sent daily, 10DLC offers businesses a reliable channel with faster delivery speeds and higher throughput. Instead of getting lost in the noise, with 10DLC, your messages stand a better chance of reaching their intended recipients promptly and efficiently.

With our industry-leading 10DLC registration and management tools, Vox Tandem can help your business integrate 10DLC into your messaging strategy. Our approvals process is swift, taking just 72 hours—a stark contrast to competitors that take up to 20 days.

Contact our team of experts to start the 10DLC approval process and start reaching more customers.

Compliance, user experience, and 10DLC campaigns

Learn how to unlock the full potential of your 10DLC campaigns through compliance and improved user experience.

Imagine a world where your Application-to-Person (A2P) messages reach users swiftly without the fear of being labeled as spam. A world where compliance with carrier guidelines doesn't feel like a chore but a pathway to achieving higher engagement rates. The world we're describing is no marketing and communications utopia but a realistic goal within your grasp.

An impactful strategy can mean the difference between success and failure in business communications. The advent of 10DLC (10-digit long code) offers businesses an opportunity to supercharge their A2P messaging. However, to truly leverage the potential of 10DLC, you'll need to navigate the intricate dynamics of compliance and user experience.

In this blog post, we'll demystify the complexities of compliance and user experience for your 10DLC campaigns. We'll explore how the strategic alignment of these two aspects can help you attain better rate limits and scores, ensuring your message not only reaches your audience but also resonates with them. Keep reading to learn how you can unlock the full potential of your A2P messaging strategy by emphasizing compliance and user experience.

Understanding the intricacies of 10DLC

A robust understanding of the 10DLC framework is crucial to leveraging its potential. You can check out one of our recent webinars for an in-depth explanation of 10DLC. But for the purpose of this article, you just need to understand that 10DLC was designed to help mitigate spam and maintain network integrity while balancing high throughput rates.

The importance of compliance in 10DLC

Because of its focus on spam mitigation and network integrity, compliance is a central aspect of successful 10DLC campaigns. Failure to comply can result in reduced message delivery rates, fines of up to $1,500 per violation, and even suspension of services. By prioritizing compliance in your 10DLC campaigns, you can sidestep those hurdles and maximize your 10DLC rate limits.

The Cellular Telecommunications and Internet Association (CTIA) provides a comprehensive set of guidelines for A2P messaging. Adhering to them is crucial for maintaining a seamless experience for users. Staying compliant includes avoiding prohibited content, following opt-in requirements, and ensuring opt-out mechanisms are in place. Organizations must also provide consistent registration and campaign information across all platforms.

Key aspects of this consistency include:

- Verifying your website domain matches your email domain
- Ensuring your brand name aligns with the one on your website
- Confirming your phone numbers are registered to your organization when searched via Google

For example, if a shoe store called Beautiful Soles wants to run a 10DLC campaign, anyone wishing to verify your numbers should be able to look them up and find them registered to Beautiful Soles, which is a division of Beautiful Soles, Inc.

Compliance measures also include:

- Presenting clear opt-in language referencing SMS or MMS on your websites—right next to the submission button
- Providing detailed campaign descriptions
- Following industry regulations
- Ensuring your messaging is consistent and transparent

It’s also critical to avoid disallowed use cases, such as:

- Any kind of unsolicited message
- Non-direct lenders
- Indirect debt collection
- High-risk lending, including third-party auto loans, mortgages, payday loans, etc.
- SHAFT (Sex, Hate, Alcohol, Firearms, or Tobacco) content
- Sweepstakes and “free giveaways”
- Cannabis

By adhering to these guidelines, you can enhance your throughput with major carriers and contribute to a better overall experience for your end users. As carriers strive to maintain high-quality user experiences and protect their networks from potential misuse, following these strict checks and criteria is essential for a smooth, reliable messaging experience.

Enhancing user experience with 10DLC

Beyond compliance, the user experience is instrumental in maximizing 10DLC scores. A superior user experience leads to more engagement, which in turn results in a higher 10DLC rate limit. There are several ways to enhance the user experience in A2P messaging:

Personalization

Personalization isn’t just about addressing users by their names. It involves understanding their preferences, patterns, and behavior to tailor messages that resonate with them. By creating personalized content, you can increase user engagement and positively impact 10DLC scores.

Timeliness

Timeliness plays a crucial role in user experience. Sending messages at appropriate times based on users' behavior patterns ensures they’re more likely to engage with your content. This proactive approach can significantly increase response rates and elevate 10DLC scores.

Clarity and brevity

In A2P messaging, clarity and brevity are of utmost importance. Messages should be concise, clear, and to the point. A well-crafted message captures the user's attention and prompts them to take the desired action.

Leveraging high-quality content

High-quality content is a vital component of strong A2P messaging strategies. Not only does it improve user engagement, but it also bolsters your compliance efforts. Good content aligns with carrier guidelines and is less likely to trigger spam filters. Furthermore, high-quality content reinforces brand reputation, encouraging users to engage more with your messages.

Here’s everything Vox Tandem customers should know about the upcoming changes and how to prepare:

- What is 10DLC? Everything you need to know
- Unregistered 10DLC is ending: What you need to know
- Your step-by-step guide to 10DLC brand registration
- SMS compliance guide and checklist
- What is A2P messaging?
- Compliance, user experience, and 10DLC campaigns
- Frequently asked questions about 10DLC

Contact our team of experts to start the 10DLC approval process and start reaching more customers.

Frequently asked questions about 10DLC

10 Digit Long Code (10DLC) Introduction & Contents

10DLC helps protect customers from unwanted spam while allowing businesses to better connect with their customers. Introduced in 2021, **10DLC has become virtually mandatory** for businesses **sending local text messaging traffic via US (+1) long code numbers** in the United States.

What is 10 DLC?

10DLC allows businesses to send application-to-person text messages (A2P) using long local codes in the United States.

Why was 10DLC introduced?

Carriers introduced 10DLC to provide a sanctioned platform for businesses to send SMS and MMS messages using long codes. Their objective is to protect consumers from unwanted spam while still allowing businesses to better connect with their customers. This change will also improve deliverability because 10DLC allows for higher messaging throughput than P2P long code traffic.

Does 10DLC allow handset receipts?

No. We recommend exploring short code or toll-free messaging if handset receipts are required.

Does 10DLC allow Free To End User programs?

No, this program is not currently available, and there are no known plans to change this.

Who 10DLC Applies To?

How do I know if 10DLC applies to me?

Generally, all traffic sent by - or on behalf of - businesses from +1 long code numbers (not Toll Free or Short Code) is governed under 10DLC. Specifically, 10DLC applies to the below types of businesses:

1. Currently sending A2P (Application to Person) traffic over long codes. Generally, all traffic sent by - or on behalf of - businesses is considered A2P.
2. A reseller or independent service vendor (ISV) with customers sending A2P traffic over long codes.

What do I need to do to comply with 10DLC?

You must:

- Register a Brand
- (optional but recommended) Vet the Brand
- Register a campaign
- Assign numbers to the campaign
- Await results of manual review
- Send traffic under those campaign numbers according to 10DLC guidelines and your specific declared Use Case(s).

Failure to do the above can result in throttled traffic, higher fees, and even fines.

Does 10DLC affect (person-to-person) P2P traffic?

According to guidelines as of 2023, virtually all SMS and MMS sent by a business—even if manually triggered by a human—is considered A2P. Therefore, while 10DLC isn't strictly required for P2P traffic, Vox Tandem has observed that most "P2P" Use Cases are often, in fact, A2P and should be registered.

You may qualify for P2P registration ONLY if the following conditions are true:

- The messages are not sent on behalf of any business or agent of a business
- You are not a cloud communication service suite
- All messages are written and sent by individuals to other individuals
- Traffic is roughly symmetrical (1:1 or 1:3 max) and, therefore, resembles normal human-to-human communication
- Your business has an excellent compliance history.
    - Note: Vox Tandem determines this history by reviewing your traffic history with us. Therefore, this process is typically only offered to long-term committed customers.

If you believe your business meets all the above conditions and qualifies for P2P Carrier Approval, please contact support to request a Carrier P2P Use Case Questionnaire.

Will toll-free numbers (TFNs) be affected by 10DLC?

No. Toll-free numbers require registration but are not explicitly covered under 10DLC guidelines. We recommend referring to our Toll-Free Messaging FAQs for more details.

How to register for 10DLC

What are the basic requirements for 10DLC registration?

10DLC requires businesses to register a Brand (business) and Campaigns (Use Cases) to increase transparency regarding who is sending what. You can submit requests to register your Brand(s) and Campaign(s) by email to support@voxtandem.com

Can I create more than one brand?

You can only create one Brand per EIN (Employer Identification Number or Federal Tax Identification Number). Additional Brands require their own unique EIN.

Can non-US brands be added while using the portal?

Yes. Please note all 10DLC rules (and possible penalties) still apply to non-US entities.

What happens after I submit my Brand and Campaign for approval?

Brand and Campaign information submitted via Vox Tandem is passed on for manual review by The Campaign Registry (TCR), the third party that administers carriers' 10DLC registration system.

In addition, Campaigns (but not Brands) are manually reviewed by Carriers. This review is an industry-wide mandatory step for all A2P 10DLC registrations.

Are any Campaigns treated differently?

Yes, the following Campaign Use Cases are treated differently:

1. Agents and Franchises
2. Carrier Exemptions
3. Charity
4. Conversational Messaging
5. Emergency
6. Political
7. Social
8. Sweepstake

These types of campaigns often require pre-approval, post-approval, and/or vetting. In some cases, they require a different vetting agent (such as Aegis or Campaign Registry for political campaigns).

This information will be displayed when transitioning from the “Use Case Selection” page.

If my campaign falls under a political Use Case, how can I be vetted for it?

Federal political campaigns can be verified via Campaign Verify or Aegis. If you did not register via Vox Tandem, you can also import the verification token they provided you with after completing their verification process.

What is the purpose of a Mixed Campaign Use Case?

A phone number can be assigned to one Campaign at most. However, a Campaign can have many assigned phone numbers.

Many businesses that want to use just one phone number register with a Mixed Use Case, which allows up to five Sub-Use Cases. A common example might be registering for a Marketing and Notifications Mixed Use Case.

Relationship between Brands, Numbers, and Campaigns

How many Brands per organization?

An EIN (Employer Identification Number) can only have one Brand assigned to it.

How many Campaigns per Brand?

A Brand can have multiple Campaigns, with a maximum of five Campaigns per Brand.

How many Numbers per Campaign?

A Campaign can have multiple Numbers. As of September 2023, the T-Mobile Limit is 49 numbers.

I have less than 49 numbers on my Campaign but was unable to add more. Why?

You may have encountered the industry’s daily number-adding limit. 10DLC intermediaries cap the amount of numbers that can be added to a given Campaign due to downstream processing constraints. We advise you to try again in one business day.

How many Campaigns or Brands per Number?

A Number can only be used in one Campaign and its parent Brand.

Brand Score, Brand Tier, and Vetting Score

What is the difference between a Brand Score and a Brand Tier?

As of mid-2023, Brand Score has been deprecated in favor of Brand Tier, which is determined by Vetting Score.

Brand Tier is used by Carriers - especially T-Mobile & AT&T to help calculate your throughput.

What is a Vetting Score, and why is it strongly recommended?

As of mid-2023, a Brand without a Vetting Score will tend to lead to low throughput for complex Campaign Use Cases like Marketing. Therefore, Vox Tandem highly recommends Vetting Scores for any Campaigns with material traffic or similarly complex compliance requirements.

Throughput - What it is and How Carriers Determine It

What is messaging throughput?

Throughput is the maximum number of messages you can send in a given period - either segments per second (MPS), per minute (MPM) or per day.

T-Mobile determines throughput as a daily messaging limit at the Brand level, meaning that all your Campaigns combined must share the daily limit.

A message segment consists of up to 160 standard characters. An SMS with more characters and/or nonstandard characters (such as emojis) can count as multiple message segments. We support up to 10 segments before messages will be rejected for being too long.

1. **Standard SMS Limit**: A standard SMS using GSM-7 encoding can contain up to 160 characters. This is the maximum size that can fit within the 140-byte (1120 bits) payload of a standard SMS.
2. **Segmentation for Longer Messages**: When an SMS exceeds 160 characters, it needs to be split into multiple segments. Each of these segments is sent as a separate SMS and then reassembled into a single message on the recipient's device.
3. **User Data Header (UDH)**: To facilitate this reassembly, each segment of a multi-part SMS must contain a header, known as the User Data Header. The UDH includes information such as the total number of segments and the position of each segment within the original message. This is necessary so the receiving device knows how to piece the message back together in the correct order.
4. **UDH Size and Its Impact**: The UDH typically takes up 7 bytes (56 bits) of the standard 140-byte SMS payload. This reduces the available space for the actual text of the message.
5. **Reduced Character Count per Segment**: When the 7-byte UDH is accounted for, the remaining space in each SMS segment is reduced. For GSM-7 encoded messages, this leaves room for 153 characters per segment (instead of the full 160).

So, in a multi-part message, each segment can only contain 153 characters due to the space required for the UDH. This is why, in practice, when you send a long SMS that needs to be segmented, each segment has a slightly reduced character limit.

How is my MPS (message segments per second) determined?

Each of your registered Campaigns will be assigned a maximum MPS based on your Brand Tier (derived from your Vetting Score) and the type of Campaign. This MPS limit is shared across all numbers attached to your Campaign and all wireless Carriers.

The same MPS limit applies whether you send all traffic through one number or split it up across multiple numbers.

Campaign Use Cases fall into four categories:

- **Declared:** Specific Use Cases. Ex., two-factor authentication (2FA)
- **Mixed:** A combination of multiple Use Cases
- **Marketing:** Marketing-related content
- **Special:** Charity, emergency, political, and other.

Declared Use Case Campaigns may receive a higher MPS than a Mixed or Marketing Campaign with the same Brand Score. However, **it is important to correctly classify your Use Case.** Incorrectly classified use cases can result in Deactivated Campaigns and hefty fines from industry organizations.

Notably, there are undeclared industry limits for MMS. As of April 2023, we estimated these to be:

	AT & T / T-Mobile	Verizon
MMS Per Second Max	0.84	25
MMS Per Minute Max	50 (per number)	

How do I register my MMS for 10DLC?

10DLC Campaigns include both SMS and MMS. While MMS throughput does not change, the carrier surcharge for MMS is higher than that of SMS.

Messaging throughput Estimate Tables

How much throughput should I expect?

Carriers have different approaches to throughput. In summary:

1. AT&T sets throughput based on Campaign. Each Campaign's throughput is determined by its AT&T "Message Class" (a score determined by Use Case and, in many cases, a Vetting Score). You typically need to Vet your brand to achieve a high score, though Russell 3000 brands may default to a high score immediately.
2. T-Mobile sets throughput based on Brand, and each Brand has a Daily Allowance
3. Verizon has not declared a method as of September 2023, though they are part of 10DLC, so following the guidelines is required to send to their customers anyway

What are the throughputs for AT&T's Message Class-based throughput system?

As of September 2023, there are over 20 categories in AT&T's throughput system, with only a few of these being in the Standard category. Use Cases in the Standard category include Dedicated (e.g., notifications), Marketing (e.g., promotions), and Mixed (e.g., an account used for promotions and notifications).

We have attempted to simplify these into the following table:

Class	Use Case	Vetting Score Requirement	TPM (SMS)	TPM (MMS)	Variable Rate depending on score
A, B	Dedicated, Mixed / Marketing	75-100	4500	2400	Y
C, D	Dedicated, Mixed / Marketing	50-74	2400	1200	Y
E, F	Dedicated, Mixed / Marketing	1-49	240	150	Y
T	Basic / Unregistered	0 / NA	75	50	N/A

There are over 15 Classes for Special Use Cases with a wide variety of throughput limits, limit methods (from per number to per Campaign), and Use Cases. Below are some of the most common Special Use Cases and their throughputs according to AT&T rules:

Message Class	Use Case	Vetting Score Reqmt	AT&T TPM (SMS)	AT&T TPM (MMS)	Variable Rate Based on Score
K	Political		4500	2400	N*
T	UCaaS Low Vol		75	50	N
B / D / F	UCaaS High Vol		240 (B) / 2400 (D) / 4500 (F)	150 (B) / 1200 (D) / 2400 (F)	Y

**Vetting is mandatory for Brands conducting political Campaigns*

What are the throughput limits for T-Mobile's Brand-based throughput

system?

T-Mobile sets limits at the Brand level, not Campaign. For Standard Campaigns, these limits are as follows:

Brand Tier	Vetting Score Requirements	T-Mobile Daily Cap
Top	75-100	200,000
High Mid	50-74	40,000
Low Mid	25-49	10,000
Low	1-24	2,000

Brands which are not Vetted and are not on the Russell 3000 may default to a Low Brand Tier for T-Mobile throughput.

What are Verizon’s throughput limits?

Verizon has not declared any throughput guidance as of September 2023. However, since Verizon has joined the TCR (the 10DLC oversight body), Vox Tandem highly recommends following 10DLC best practices.

10DLC Definitions / Acronyms

- **10DLC:** 10 Digit Long Code. The protocol under which local long code A2P messages are regulated in the United States
- **A2P:** Application To Person Messaging. This typically covers ALL messages sent by or on behalf of a business.
- **Brand:** The trading name of the company sending messages to a customer
- **Campaign:** A way to organize 10DLC-registered numbers and their use cases, as governed by the TCR
- **MO:** Messaging Origination. A message sent to an A2P number. An MO fee determines the charges Carriers apply for receiving messages from one of their customers.

- **MT:** Messaging Termination. A message sent from an A2P number and terminating on and end user's handset. MT fees determine the charges Carriers apply for sending to their customers.
- **P2P:** Person-to-person. Messaging that is sent manually from one person's phone to another, and is not on behalf of a business. P2P is subject to some special exemptions, but as a general rule Vox Tandem notes that ALL messages sent by businesses are considered A2P
- **TCR:** The Campaign Registry, an entity appointed by the Carriers to manage 10DLC registration records.

Here's everything Vox Tandem customers should know about the upcoming changes and how to prepare:

- What is 10DLC? Everything you need to know
- Unregistered 10DLC is ending: What you need to know
- Your step-by-step guide to 10DLC brand registration
- SMS compliance guide and checklist
- What is A2P messaging?
- Compliance, user experience, and 10DLC campaigns
- Frequently asked questions about 10DLC

Contact our team of experts to start the 10DLC approval process and start reaching more customers.

SMS compliance guide and checklist

SMS, or text messaging, is a simple, effective marketing tool that helps businesses communicate with consumers. However, strict regulations dictate how and when businesses use SMS, and there are significant penalties for getting it wrong. In addition to damaging your reputation, violating these regulations can result in hefty fines: the average cost of a Telephone Consumer Protection Act (TCPA) lawsuit was $6.6 million in 2019.

Below, we give you a detailed guide to SMS compliance along with tips to ensure your SMS campaign is compliant:

SMS regulations and compliance

SMS regulations ensure that consumers only receive SMS communications they have consented to receiving. They mandate simple opt-out processes and consumer data protection laws, among other things.

Applicable regulatory organizations

SMS rules and regulations are built on a foundation laid by the General Data Protection Regulation (GDPR) in Europe and the Telephone Consumer Protection Act (TCPA) in the U.S.

In general, the aim is to protect end users from receiving unsolicited or unwanted messages via SMS. The penalties for getting it wrong can include an immediate shutdown of service or fines ranging from $500 to $1,500 per message. The first step toward compliance is understanding the regulations outlined by the GDPR and the TCPA.

GDPR

The General Data Protection Regulation (GDPR) is the European Union's set of consumer data protection laws. Fines are based on business revenue, and can be up to 20 million Euros or 4% of a business's global revenue. The GDPR is one of the strictest sets of data protection laws, and has three core principles: consumer consent, opt-out information and customer data management.

Consumer consent: consumer permission, preferably provided in writing, is necessary before you can contact an individual through any channel. Opt-out information: organizations must include opt-out links or keywords in every piece of communication. Customer data management: sharing data with third parties and other companies is prohibited, unless consent has been given by the customer beforehand. While data encryption is not explicitly required, it's a best practice because businesses can be held liable in the event of a data breach if measures weren't taken to protect consumer data.

TCPA

The Telephone Consumer Protection Act (TCPA) is enforced by the Federal Communications Commission (FCC), a U.S. government agency that oversees television, radio and phone communications. The TCPA is the U.S. equivalent of the GDPR.

Each non-compliant call or text message counts as a violation, and fines can cost anywhere from $500 to $1500 per violation. Furthermore, class action lawsuits can be filed under the TCPA—businesses can be fined for multiple violations for every customer affected. The main focus of the TCPA is customer permission and identifying automated communication.

Customer permission: similar to the GDPR, the TCPA states that you must receive permission from customers before contacting them and primarily emphasizes SMS, calls and email. Identify automated communication: it is required that you tell customers if you are contacting them through an automated system, so this must be specified when collecting consent.

CTIA

The Cellular Telecommunications Industry Association (CTIA) isn't an enforcement agency, but it gives guidance for businesses using SMS. The CTIA is made up of major mobile carriers in the U.S. and it creates a list of best practices for the SMS marketing industry. The primary goal of these best practices is to ensure that consumers are protected from unwanted messages and that consumers can exchange wanted messages with organizations and with other consumers.

PIPEDA

The Personal Information Protection and Electronic Documents Act (PIPEDA) is the set of consumer data protection laws enforced by the Office of the Privacy Commissioner of Canada. Although similar to the GDPR and TCPA, PIPEDA has some unique requirements, including identifying purposes and limiting collection and use.

Identifying purposes: you must receive consent before contacting customers, and you must also explicitly explain why you are asking for a phone number or email address. Limiting collection and use: you can only collect and store customer information necessary for a specific purpose.

MMA

The Mobile Marketing Association (MMA) is a nonprofit trade organization made up of over 800 global companies that use SMS marketing. Like the CTIA, it is not a regulatory body, but instead encourages companies to adhere to a framework that protects brand image and reputation. The MMA is a think-tank style organization that encourages members to participate in marketing events, committees and research to develop best mobile marketing practices.

FTC

The Federal Trade Commission (FTC) is a federal agency in the U.S. that enforces laws and oversees consumer complaints of violence, fraud and identity theft. Its goal is to prevent businesses from engaging in deceptive and unfair practices that would harm consumers or other competing businesses.

The FTC is the law enforcement that cracks down on businesses in violation of the rules set by other U.S.-based agencies (like the TCPA created by the FCC). The FTC collects complaints from consumers and responds by levying legal action and/or fines against businesses..

The FTC also manages the Do Not Call Registry - a list of individuals who do not want to receive marketing communications from businesses. It’s illegal to contact anyone on the Registry with unsolicited texts or calls.

SMS compliance checklist

1. Obtain express written consent before beginning communications

You must receive explicit written consent before sending SMS messages to consumers. That consent must be documented and saved, otherwise you risk fines of $500-$1500 per message. Written consent can be obtained by asking a consumer to submit their information via a paper or online form, click a checkbox on a website or text a short keyword to your campaign phone number.

2. Provide a clear opt-in and disclose details

After obtaining written consent you must send an opt-in message (also known as a call-to-action message) reminding consumers that they have consented to receive communications from your organization. That first message should make the following clear:

- Your organization's name and purpose
- How often consumers will receive texts
- Message and data rate notices
- Messaging campaign terms and conditions (or a link to these details)
- Opt-out instructions

3. Confirm the opt-in and remind subscribers of terms and conditions

After the initial disclosure text, it's good practice to confirm the receiver's opt-in and send another reminder of your terms and conditions in case they've forgotten that they signed up. You should also notify consumers via text whenever the terms and conditions change. This confirmation text could come before or immediately after your first marketing message.

4. Time your communications appropriately

According to the TCPA, businesses cannot text or call consumers before 8:00AM or after 9:00PM. Ensure your communications are timed so that consumers, wherever they are located, receive messages within that time range to avoid complaints and fines.

5. Include your organization’s name in each message

Make sure to include your organization’s name in each message to maintain transparency and eliminate consumer confusion. Consumers should always be able to recognize who is messaging them and why.

6. Avoid prohibited language

The CTIA’s rules impact the type of content businesses can include in text marketing messages. Use the acronym SHAFT to remember what type of content is not allowed: SHAFT stands for Sex, Hate, Alcohol, Firearms and Tobacco. If your marketing message includes content around these topics, your business risks high fines and permanent bans.

Of course, there are a few exceptions to this rule. For example, if your business is in the restaurant industry, you may be allowed to promote happy hour specials. However, there are additional requirements for marketing campaigns of this nature—anything alcohol-related requires additional safeguards, like preventing underage user signups.

7. Offer a way to opt out

Customers should be able to unsubscribe from your marketing messages easily. It’s important to send opt-out instructions often to remain in compliance. One way to do this is to set up “STOP” response capabilities—then simply include a brief reminder at the end of each marketing message.

8. Respect opt-outs and the Do Not Call Registry

If a consumer opts out, it’s illegal to continue to text or call them about your marketing communications. You can send one final message confirming that they have successfully opted out, but that’s it. It’s also important to note that contacting anyone on the National Do Not Call Registry is illegal as well, and can result in hefty fines.

How to write a compliant SMS message

Let’s take a look at what it means to be compliant in your SMS marketing messaging. Here are some examples of what your marketing messages should look like:

DOs and DON'Ts of obtaining written consent for SMS compliance example

- You must obtain written consent via form, checkbox, or text keyword before messaging consumers.
- You must give consumers the opportunity to opt into communications and disclose details of your messaging campaign.
- Make sure the consumer knows what organization is contacting them.
- Give consumers an easy way to opt out of future messages.

Which number type works best for your SMS content

When it comes to business messaging, there are several number types available, each with its own set of rules.

Long codes are 10-digit phone numbers designated by mobile operators for Person to Person (P2P) communication. They are for non-marketing communications only, so appropriate use cases include chat applications and customer service.

Short codes are five- or six-digit phone numbers that customers can lease from the Common Short Code Administration. Users need to opt into this type of message. Short codes are most commonly used for nonprofit fundraising campaigns, password resets and alerts.

Toll-Free numbers are numbers with distinct 3-digit codes (e.g., 800, 888, 877, etc.) that are often used for customer service use cases. Regardless of where they’re calling from, callers can dial a toll free number without incurring long distance charges. Unlike short codes, toll-free numbers support both phone calls and SMS, so customers can respond to communications from a toll-free number by texting or calling the number back. Example use cases include appointment reminders, account notifications and emergency alerts.

Get compliant and learn more

Set up a call today with one of our experts to discuss SMS compliance, laws and regulations in depth. Then get started with your SMS campaign by purchasing a long code, short code, or toll free number.

This guide, checklist and our experts serve as a comprehensive overview of what you need to know, but it's not a replacement for qualified legal counsel.

Here's everything Vox Tandem customers should know about the upcoming changes and how to prepare:

- What is 10DLC? Everything you need to know
- Unregistered 10DLC is ending: What you need to know
- Your step-by-step guide to 10DLC brand registration
- SMS compliance guide and checklist
- What is A2P messaging?
- Compliance, user experience, and 10DLC campaigns
- Frequently asked questions about 10DLC

Contact our team of experts to start the 10DLC approval process and start reaching more customers.

Quick Guide to 10DLC - Everything you wanted to know!

Unregistered 10DLC is ending: What you need to know

Unregistered 10DLC traffic is coming to an end. Find out what actions you need to take to remain compliant.

The landscape for 10-digit long code (10DLC) messaging has undergone significant regulatory shifts. US carriers will officially cut off all unregistered 10DLC traffic on **December 1, 2024**. This deadline marks the end of unregistered traffic on US 10DLC routes. Businesses that rely on unregistered numbers for messaging need to take immediate action to remain compliant and avoid service interruptions.

Here’s everything Vox Tandem customers should know about the upcoming changes and how to prepare:

- What is 10DLC? Everything you need to know
- Unregistered 10DLC is ending: What you need to know
- Your step-by-step guide to 10DLC brand registration
- SMS compliance guide and checklist

- What is A2P messaging?
- Compliance, user experience, and 10DLC campaigns
- Frequently asked questions about 10DLC

Contact our team of experts to start the 10DLC approval process and start reaching more customers.

eFax Management - Report Access Changes

Removal of Reports Notification

We'd like to remind you of the upcoming changes to report availability in the eFax Management portal as part of our ongoing efforts to enhance your experience:

Report Access Changes:

1. **Starting February 19th,** the following reports will no longer be accessible in the portal:
   - Summary Report
   - Billing Report
   - Fax Machine Connectors Orders Report
   - Grouped Stats By Number Report
2. **Starting April 23rd,** the following report API endpoints will no longer be accessible:
   - Summary Report
   - Billing Report

Enhanced Recommended Replacements:

- To replace **Summary Reports**, please use:
  - Usage Total Report
  - Usage By Account Report

- To replace **Billing Reports**, please use:
  - Usage Total Report
  - Accounts Total Report
  - Users Total Report
  - Numbers Total Report
  - FMC Total Report

We encourage you to explore these alternatives to ensure a smooth transition. Should you have any questions or need assistance, feel free to reach out to our support team at support@voxtandem.com