WHITEPAPER

Guide to U.S. Messaging Compliance

Updated with July 2019 CTIA Guidelines

BEST PRACTICES FOR BUSINESS

Knowing who, what, how, and when to message consumers in the United States can be challenging. The business SMS messaging ecosystem is complex and can easily seem overwhelming. Sending a message to the wrong person at the wrong time may not only affect your customer's experience but could also put your business at risk of legal action. Buzzwords like opt-in, opt-out, P2P, A2P, TCPA, and CTIA can make the idea of sending messages to customers that much more daunting. On the other hand, a welcome text message to the right person can be a powerful and effective way to communicate with your users.

Twilio is here to help. In this whitepaper, we've compiled SMS best practices from the newest edition of CTIA guidelines and the Telephone Consumer Protection Act (TCPA) regulations, which provide helpful guidance and industry practices for how to engage your customers. We've also embedded our expert experience to help you determine your compliance strategy when sending messages to your end-users. Throughout this guide, we'll use SMS and messaging interchangeably, though these guidelines also apply to other forms of digital messaging like Rich Communication Services (RCS) and Multimedia Messaging Services (MMS).

Keep in mind, we aren't your lawyers, so we aren't at liberty to give you or your organization legal advice. This whitepaper represents Twilio's interpretation of messaging best practices as of the date of publication. Please note that compliance with legal frameworks, such as the TCPA, may depend on your particular use case and will likely be fact and context-specific. The information contained in this whitepaper should not be relied upon as legal advice or to determine how CTIA guidelines or the TCPA requirements apply to your use of messaging. We encourage you to seek guidance from your legal counsel with regard to how these frameworks apply specifically to your business or organization and how to ensure compliance. This information is provided "as-is" and may be updated or changed without notice. You may copy and use this content for your internal, reference purposes only.

Executive summary

The underlying purpose of both the U.S. regulatory and telecommunication industry rules that govern businesses' and organizations' use of messaging to communicate with users is to ensure that people do not receive communications that they do not want to receive. Put another way, people should only receive messaging communications they want to receive from businesses or organizations.

As a business or organization, it only makes sense that this is (and should be) your goal as well—to send communications to individuals who want to receive them. For the same reasons that SMS is an effective mode of communication (i.e., 98% of received SMS are read by the recipient), unwanted communications are a source of irritation. Sending unwanted SMS is both a waste of time and resources and is likely to irritate people, resulting in potential damage to your organization's brand. A 2019 Twilio and Lawless Research study found 75% of Gen Z/Millennials took one or more negative actions when businesses did not meet their communication preferences. [1]

So, when thinking about building a compliant SMS campaign, remember first the underlying goal of the compliance frameworks: to protect people against unwanted communications.

Of course, whether a message is unwanted or not, is in the mind of the recipient. This is where the best practices outlined in this whitepaper can help. These best practices outline the industry standards that help organizations to ensure that the messages they send are wanted by the people receiving them, and in the process, ensure that they are in compliance with regulatory and industry requirements.

This whitepaper will cover:

- **Calls to Action:** When messaging your customers, it's imperative to display clear calls to action while requesting your customer's phone number. You should always tell consumers exactly what they are signing up to receive. This guide provides step-by-step instructions to help ensure you are operating within accepted guidelines, regardless of the number you are using to send SMS messages.
- **Opt-in Mechanisms:** First and foremost, always offer transparent opt-in mechanisms. Consumers must consent clearly to receive all messages; simply entering a mobile phone number does not necessarily constitute a compliant opt-in. Be sure to send an opt-in confirmation message when you send your first message. For recurring messages programs, confirmation messages must include clear opt-out instructions. Businesses should also remind consumers, from time to time, that they are still enrolled.
- **Honoring Opt-Outs:** Always respect and acknowledge opt-out requests. Regardless of whether you are using long code, toll free numbers, short codes, or some other means of messaging, senders must acknowledge and act on all opt-out requests. Failure to do so can put your business at risk of legal action. Twilio is not responsible for any action taken against a business due to messaging complaints.

This guide provides best practices and examples to make this process easy. Note that there may be additional regulatory or industry best practice considerations depending on your use case or industry. And, if you're sending messages outside of the United States, you will want to review additional regulatory information at twilio.com/guidelines. You should consult with your legal counsel to ensure your use case is compliant with all applicable laws and frameworks, including TCPA requirements and CTIA guidelines (we'll explain more about these laws and guidelines in the next section).

Background

First, let's discuss the two main governing frameworks that affect how you send messages to consumers in the United States.

The Telephone Consumer Protection Act (TCPA) is a federal statute enacted in 1991, designed to safeguard consumer privacy. This legislation places restrictions on telecommunications via voice calls, SMS texts, and fax. The intent of the TCPA is to empower consumers to decide which auto-dialed calls and text messages they receive and to prevent receipt of unwanted auto-dialed calls and text messages. It is important to note that violations of the TCPA carry a hefty penalty—allowing aggrieved consumers to sue for damages of $500 per call or text message or $1500 per call or text message if the violation was knowing or willful.

[1] Twilio Inc & Lawless Research. (2019). *The Authenticity Gap.*

CTIA is a trade association representing the wireless communications industry in the United States, including wireless carriers, suppliers, manufacturers, and providers of wireless products and services. CTIA exists as the voice and guidance of the wireless industry in the United States. Their primary responsibilities are advocating for legislative and regulatory policies and helping to create industry-wide standards for messaging and other wireless products with which we interact on a daily basis.

You may be wondering if you should follow CTIA's guidelines if they aren't legally binding. The answer is simple—yes. These guidelines were created through consultation with industry stakeholders and aligned with TCPA requirements to ensure consumer protection. The guidelines were also developed to ensure that individuals are able to receive the messages they want, either from other individuals or from organizations. They were created specifically for those organizations and individuals looking to send Application-to-Person (A2P) traffic over the wireless networks. Recent updates to CTIA's guidelines put a finer point on what is considered A2P traffic and provide new guidelines for how businesses should message with their customers over SMS (Short Message Service), MMS (Multimedia Message Service), and RCS (Rich Communication Services).

Following these guidelines will not only protect your organization but will offer your customers the best experience when interacting with your organization and brand. Furthermore, with the Federal Communications Commission (FCC) and Federal Trade Commission (FTC) reporting millions of complaints from consumers regarding unwanted calls and messages each year, the regulatory and industry pressure to protect consumers from unwanted text messages is only likely to increase.

P2P vs. A2P

The first step in ensuring you provide a compliant and contextual messaging experience for your end-users is knowing the difference between Person-to-Person (P2P) and Application-to-Person (A2P) messaging. In the 2019 CTIA Best Practices, P2P was updated to refer only to Consumer messaging, and A2P to refer to any Non-Consumer messaging.

CTIA defines messaging interactions in two distinct ways:

Consumer (Person-to-Person (P2P)) and Non-Consumer (Application-to-Person (A2P)).

P2P is defined by CTIA as the low-volume exchange of wireless messages (SMS, chat, etc.) between individuals. Notably, CTIA has updated the definition of a consumer to exclude employees or agents of businesses or organizations sending messages to consumers. Under the updated best practices, P2P consumer messaging is limited to wanted messages between two consumers, like the kind one might send to a friend or family member.

A2P is defined by CTIA as all traffic that falls outside normal consumer-to-consumer interactions. This includes conversational messages with a support team, or a sales rep, as well as marketing messages, political messages, advocacy messages, appointment notifications, IT alerts, and other types of calls to action. A2P traffic is a focus area for regulators and carriers alike in today's messaging landscape.

Note: For proxied conversations, where a Twilio phone number sits between the individuals communicating, it's important to disclose to your consumers that this is occurring. This is commonly done in the company's Privacy Policy. Common examples of a proxied conversation are a rider interacting with a driver to coordinate a point of pickup, or a delivery driver communicating with the delivery recipient. If you'd like more information, Twilio offers best practices for managing communications and records between users.

Number Types

Now that you know the difference between P2P and A2P traffic, you need to understand the types of phone numbers. Different types of phone numbers provide customers with different options for both P2P and A2P traffic, and each comes with different benefits and risks. More than 26 billion SMS are sent every day and some messages are intended for A2P infrastructure which supports the higher throughput required for business messaging.

In North America, Twilio offers three types of numbers for SMS messaging: short codes, long codes, and toll-free numbers. Each type of number offers different benefits in terms of throughput, cost, ease-of-acquisition, and how effective they are at sending A2P traffic.

Short codes are five- or six-digit phone numbers (ex. 234546) which are leased through Twilio's Console annually or quarterly. You can select a random short code or a vanity short code, which is a short code number that you choose to suit your business or organization. You can find out if the number you want is available by searching the Short Code Registry.

Short code numbers go through an eight- to twelve-week approval and screening process with the carriers, which allows their traffic to avoid any potential filtering. Additionally, while short codes are capable of sending messages at a higher throughput than any other type of phone number, U.S. short codes can only send messages to U.S. phone numbers. Nonetheless, this is a must-have for any fully-scaled A2P use case where you will send large volumes of messages. On the other hand, short codes may feel less personal for conversational use cases. It's worth noting that CTIA periodically audits short codes to ensure the usage matches what was submitted during the approval process.

Long codes are 10-digit phone numbers (ex. 415-234-5618) which are provisioned through Twilio's API or Console, and billed monthly. Long code numbers are often instantly provisionable, and can be used immediately to send messages. They can also provide a more localized and personal-feeling customer experience when sending messages.

There are some limitations to long code numbers: long codes can only send at a rate of one message per second and messages sent from them can be filtered at the carriers' discretion. However, with the addition of A2P 10-Digit Long Code routes (10DLC) to the U.S. carrier ecosystem, businesses may be approved for additional throughput on 10DLC numbers through additional vetting and verification.

Long term, if you are sending messages to people both inside and outside the U.S., we recommend using a U.S. short code for your U.S. subscribers, along with toll-free numbers or non-U.S. short codes (where available) for communicating with your non-U.S. subscribers.

Toll-free numbers are 10-digit phone numbers (ex. 800-234-5618) which may also be purchased through Twilio's API or Console, are billed monthly. Like long codes, these numbers can be used immediately and are another option for businesses looking to send messages while they wait for a short code for their A2P use case. These can send at a rate of three messages per second (MPS), although there are options for increasing throughput to 25 MPS with High Throughput Toll-Free. Messages sent from toll-free numbers can be filtered at the carriers' discretion, just like long codes.

As you can see, there are compliance, throughput, and provisioning considerations for each number type. Regardless of the number(s) you're using to send messages, opt-ins are a mandatory component of any messaging flow.

The Opt-Ins and Outs of Messaging Consumers

Because the goal of a compliant campaign is to send communications to consumers or constituents that they want to receive, handling opt-ins and opt-outs properly is fundamental. Under the new CTIA guidelines, A2P messaging requires consent from consumers, with the type of consent (implied, explicit, or written) varying by use case.

An **opt-in** is the consumer's consent to receive messages. It is the most straightforward way to determine whether the messages you intend to send to the consumer are wanted—you ask them. However, just as in everyday life, the way you ask the consumer if they want to receive your messages matters. The goal is to ensure that you and the consumer have a "meeting of the minds" as to whether that consumer wants to receive the messages you intend to send. To ensure there is a "meeting of the minds," opt-ins should be contextual and timely.

Think of this in terms of campaigns: consumers should be opting in to specific messages for a reasonable period of time. For example, a voter who opted-in for one election cycle does not necessarily indicate an opt-in for the next one. Customer experience is affected when messages are sent for reasons other than the ones consumers signed up for and when messages are sent long after the consumer remembers opting in to receive the messages.

In addition, under the TCPA, certain opt-ins, such as for automated SMS marketing messages, must be logged in some form of writing—whether that writing is done by electronic means, or old-fashioned pen and paper. The updated CTIA best practices support this approach to ensuring messages are wanted, requiring express consent to receive messages and written consent to specifically receive promotional messages. However, whether your messages are promotional or otherwise, we recommend that all opt-ins be documented in some way so that you can demonstrate how and when you received the consumer's consent to send him or her messages.

To remain compliant, and to minimize risk related to customer complaints, we further recommend establishing a double opt-in. Once a consumer signs up to be messaged, remind them that they signed up with their first message, then have them respond with their consent to begin the messaging campaign. This is not always necessary, but it is an industry best practice.

Opt-outs are the revocation of consent from the consumer to receive a message. Commonly, this is done by replying 'STOP' to a message, but can expand to other reply language or opting out via web forms, voice calls, and other means of communication captured by a business. The FCC determined that consumers should be able to opt-out through "any reasonable means." Accordingly, you should be careful to not unreasonably restrict how consumers can express their desire to opt out of further messages. The definition of "reasonable means" is contextual and will be dictated by the nature of your use case and business.

Ultimately, opt-ins are always required—double or not—and, respecting a consumer's choice to opt-out, no matter how expressed, is a must. There are real business risks for sending messages without consent, with Twilio, CTIA, and under the TCPA.

Types of Opt-Ins

As noted in the previous section, obtaining a clear opt-in from consumers before you message them is a key component of a successful SMS campaign. Here are some examples of various types of opt-ins for different use cases:

Handset Opt-In

Your consumers might see a short code or other phone number marketed somewhere, like a sporting event, billboard, or website which asks the consumer to text a phone number in order to opt in. There are many uses for this type of opt-in, including: giveaways and promotions, beginning a support conversation, and different kinds of notifications and updates.

Example

Recipient: {Keyword}

Short code: Welcome to {Campaign Name} {Description} Alerts! Msg&data rates may apply. {Message frequency} Reply HELP for help, STOP to cancel.

Note: The "description" should be a single word to define the kind of alerts, e.g. "Account Alerts," "News Alerts," "Promo Alerts," etc. The message frequency must be specific, but can be any interval, for example: "1 message per day," "4 messages per month," "2 messages per transaction," etc. If the message frequency will vary based on user interaction, "1 message/user request" is standard.

Non-Handset Opt-In

Non-Handset Opt-ins occur through different types of consumer action outside of sending an SMS. Consumers may opt in to support assistance through a web form or app, an IVR/phone tree, or during a purchase through a point of sale (POS) device.

Web, App, or Paper Forms

Your consumers might opt-in to receive messages when they give their mobile number to a website, mobile app, or paper form, or otherwise without using a handset.

Example

While no longer required under CTIA guidelines for recurring message programs, we still recommend that when a recipient initially signs up by any means other than from a mobile handset, a double opt-in process is used. The message flow might look like this:

Recipient signs up without using mobile handset, such as on a web form, and receives a text message from the short code asking to confirm the opt-in.

Short code: Text YES to join {Campaign Name} {Description} Alerts. Msg&data rates may apply. {Message frequency} Reply HELP for help, STOP to cancel.

Recipient: YES

Short code: Welcome to {Campaign Name} {Description Alerts! Msg&data rates may apply. {Message frequency Reply HELP for help, STOP to cancel.

Note: Rather than confirming the opt-in with a text message keyword such as YES, recipients may confirm by entering a verification code online instead. Once the verification code has been entered, a compliant welcome message must be sent to the handset.

IVR Opt-In

There are a few newer types of opt-ins we are seeing in the market. More and more consumers are opting in via an interactive voice response (IVR)/phone tree.

These opt-ins can occur when a contact center's reps are overloaded and there are high hold times. The consumer has an option to "Press 1" to begin a messaging support conversation.

Example

Recipient inputs a digit in the IVR call flow and then receives a text message from the short code asking to confirm the opt-in.

Recipient: YES

Short code: Welcome to {Campaign Name} {Description} Alerts! Msg&data rates may apply. {Message frequency} Reply HELP for help, STOP to cancel.

Short code: Text YES to join {Campaign Name} {Description} Alerts. Msg&data rates may apply. {Message frequency} Reply HELP for help, STOP to cancel.

Note: As with the traditional non-handset opt-in, rather than confirming the opt-in with a text message keyword such as YES, recipients may confirm by entering a verification code online instead. Once the verification code has been entered, a compliant welcome message must be sent to the handset.

Point of Sale (POS) Opt-In

A POS opt-in occurs after a purchase is made, generally in a brick and mortar location. A typical workflow is when consumer completes their purchase and wants to opt in to a loyalty rewards program or receive their receipt via text.

Example

Recipient inputs their phone number into the point of sales hardware post-purchase and then receives a text message from the short code asking to confirm opt-in.

Short code: Text YES to join {Campaign Name} {Description} Alerts. Msg&data rates may apply. {Message frequency} Reply HELP for help, STOP to cancel.

Recipient: YES

Short code: Welcome to {Campaign Name} {Description} Alerts! Msg&data rates may apply.

How Twilio Handles Opt-Outs for Different Number Types

By default, Twilio handles standard English-language reply messages such as STOP, STOPALL, UNSUBSCRIBE, CANCEL, END, or QUIT for toll-free and long code messages, in accordance with industry standards. Supported opt-out and opt-in keywords for Twilio Programmable Messaging are listed below.

As global regulations vary by country and region, we now support language and country overrides for number pools through the Advanced Opt-Out service in Messaging Services, allowing you to add non-English, or non-standard keywords in addition to universal keywords.

Long Codes

For long code messages, Twilio handles opt-outs for the following replies: STOP, STOPALL, UNSUBSCRIBE, CANCEL, END, or QUIT. Any future messages will error out with the error code 21610 and fail to send to consumers that have opted-out, automatically. You can track delivery and opt-outs of SMS in real-time using status callback urls. Alternatively, you can use the API to query your logs for messages that contain these opt-out keywords in the body, like STOP or using the OptOutType parameter included on your configured webhook URL in Messaging Services. Regardless of how your organization monitors opt-outs, it's critically important to comply with their request.

Users can always opt back in by replying START, YES, and UNSTOP (keywords are not case sensitive).

While Advanced Opt-Out for Messaging Services supports many of the intricacies of a customized compliance lifecycle for most businesses, customers can choose to manage their own long code opt-outs by submitting a request to Twilio's support team.

Short Codes

Twilio does not handle opt-outs for short code phone numbers on behalf of our customers by default. As part of the application process for obtaining a short code, the applicant must document their intended opt-out process and flow. We've found that businesses and organizations that go through this application process will want control of creating and maintaining a blacklist of those customers that have opted out of receiving future messages in order to create a more branded opt-in/out experience, remain compliant with Twilio's acceptable use policy and CTIA guidelines, and to avoid any legal risk to their business. A how-to guide on how to manage opt-outs on short codes can be found in this article.

Note: For recurring short code campaigns, be wary of numbers that may no longer belong to the previous owner. Sometimes numbers are moved from one consumer to another without much notification. It is important when sending messages for recurring campaigns to periodically confirm with consumers that the number they provided is still their number. This can be done in a few ways: periodically using Twilio's Caller Lookup to confirm the owner of the phone number is the same, or by sending an email or in-app push message to the consumer, prompting them to confirm that the number is still their phone number.

Conclusion

A great messaging experience will delight your customers or supporters and is key to delivering great customer engagement. Regardless of the channel or number types you choose, these guidelines and best practices will not only help mitigate potential legal risk but will enhance your customers' experience as they interact with your brand.

Remember to ensure that all users you're messaging have opted-in and that they can opt out at any time. Make your messages contextual and timely. Don't overstay your welcome in customer's inboxes, and remember that every customer is an advocate for your brand wherever they go. Make their experience with your company magical!

Questions, comments, or concerns? Get in touch with our Support Team.

Additional Resources:

- TCPA
- CTIA Short Code Monitoring Hand book
- CTIA Messaging Principles and Best Practices
- Twilio Acceptable Use Policy
- Managing SMS between your users

Published October 2019