Version: 3.3
Updated: 1 7 22

Twilio's guide to US messaging compliance

About this e-book

Knowing who, what, how, and when to message consumers is increasingly complex as they've become more selective about how they interact with their devices.

SMS messaging is now the cornerstone of internal and external communication strategies for many businesses. But buzzwords like *opt-in*, *opt-out*, *P2P*, *A2P*, *TCPA*, *10DLC*, and *CTIA* can feel like gatekeepers to developing a messaging plan. And sending a message to the wrong person at the wrong time may not only impact the customer's view of your brand, but could put a business at risk of legal action. However, a welcomed and meaningful message sent to the *right* person at the *right* time can lead to a significant positive impact to your business.

Twilio is here to help you wade through the complexities of the SMS messaging space. Within this e-book, we have outlined the key regulations and guidelines required for the business SMS messaging space. Best practices are based on industry guidelines and the Telephone Consumer Protection Act (TCPA), and are compiled in the Twilio Messaging Policy.

We have also included our expert guidance around these policies to enable you to create the best compliance strategy for your business. 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 guide 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 e-book 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 regarding 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.

Contents

Executive summary

The underlying purpose of both the U.S. regulatory and telecommunication industries' rules governing how businesses and organizations use messaging to communicate with users is simply to ensure that people receive only messaging communications they want to receive and not those they do not want to receive.

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 a waste of both time and resources, and is likely to lead to unhappy consumers, resulting in potential damage to your organization's brand and customer engagement efforts. 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 building a compliant SMS campaign, remember the underlying goal of the compliance frameworks: to protect people against unwanted communications. You send messages for a reason, whether it is a one-time passcode, a critical alert, supporting a marketing campaign, or a pre-sales conversation. Those messages only achieve their

1: Twilio Inc & Lawless Research. (2019). The Authenticity Gap.

75% of Gen Z/Millennials took one or more negative actions when businesses did not meet their communication preferences.[1]

Twilio Inc & Lawless Research. (2019). The Authenticity Gap.

intended purposes when they reach and are ultimately read by the consumer, so all these policies are designed to ensure the messaging channel is trusted and delivers the expected business outcome.

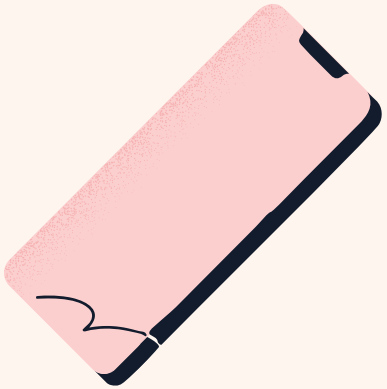
Of course, only the recipient can decide if a message is wanted. This is where the best practices in this guide can help: by walking you through the industry standards that help organizations ensure the messages they send are wanted by the people receiving them while complying with regulatory and industry requirements.

This guide will cover:

- **Calls to action:** How to clearly articulate your intentions behind SMS communications and the types of messages consumers will be receiving from you, while operating within the accepted legal guidelines.
- **Opt-in mechanisms:** Offering consumers direct and simple ways to opt in to your messaging communications with clear consent.
- **Honoring opt-out:** Ways to respect and acknowledge opt-out requests to remain compliant with CTIA and TCPA guidelines, and avoid legal risks. This applies to all phone number types, including short codes, local long codes, and toll-free numbers.

The best practices and examples in this guide are intended to make this process easy, but note that there may be additional regulatory or industry best practice considerations depending on your use case or industry. If you're sending messages outside of the U.S., you will want to review additional regulatory information here. 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, which we'll explain in the next section.

Background



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

TCPA is a federal statute enacted in 1991, designed to safeguard consumer privacy. This legislation places restrictions on telecommunications that happen 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 $1,500 per call or text message, if the violation was knowing or willful.

CTIA is a trade association representing the wireless communications industry in the U.S., 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 U.S. Its primary responsibility is advocating for legislative and regulatory policies, and helping to create industry-wide standards for messaging and other wireless products.

While CTIA's guidelines aren't legally binding, they were created through consultation with industry stakeholders and aligned with TCPA requirements to ensure consumer protection, so they do need to be followed. The guidelines were created specifically for those organizations and individuals looking to send Application-to-Person (A2P) traffic over the wireless networks and ensure individuals can receive the messages they want, either from other individuals or from organizations. 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).

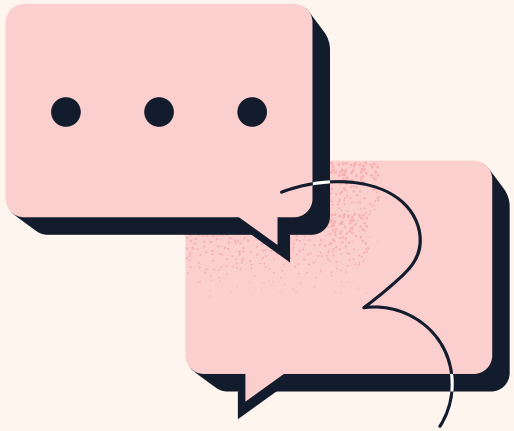
Following these guidelines will not only protect your organization, but will also offer your customers the best experience when interacting with your organization and brand. And with the Federal Communications Commission (FCC) and Federal Trade Commission (FTC) reporting millions of complaints from consumers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

Twilio messaging and acceptable use policy

Twilio partners with organizations that want to engage with their consumers in meaningful and deliberate ways, so staying compliant is of utmost importance.

The CTIA guidelines and TCPA requirements were written to protect consumers from unwanted and unlawful messaging activities in the U.S. Since business today is international, we've consolidated a list of rules, regulations, and forbidden message categories (these apply to both brands and independent software vendors) into the Twilio Messaging Policy and Twilio Acceptable Use Policy, to help you stay compliant wherever your end users might be.

P2P vs. A2P



The first step in ensuring you provide a compliant and relevant 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 Messaging Principles and 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. It is important to note that the 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 only 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 the normal consumer-to-consumer interactions. Think 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. All Twilio traffic is defined as A2P.

Note: For proxied conversations, meaning that 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.

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 (e.g., 234546) that 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. It's worth noting that CTIA periodically audits short codes to ensure the usage matches what was submitted during the approval process. Along with the CTIA audits, Twilio also conducts its own audits to ensure compliance and to assist with any required application adjustments.

Short code numbers go through a six-to-10-week approval and screening process with the carriers—which allows their traffic to experience the highest possible delivery volume—and are especially well suited to transactional messages, such as a weather alert to a community or any notifications with critical deliverability needs. However, short codes can only send to U.S. phone numbers and can feel less personal if the intent is to have a conversational campaign, if you expect or want a reply.

Note: Shared short codes—or single short codes that are being used by multiple businesses or brands at the same time—cause spam reports and increased filtering across the U.S. and Canada. Shared short codes are now forbidden by major carriers for any messaging purposes.

Local long codes are 10-digit phone numbers (e.g., 415-234-5618) that are provisioned through Twilio's API or Console and billed monthly. Long code numbers are often instantly provisionable, meaning they can be used immediately to send messages. Originally, local long codes were intended to be used for P2P messaging rather than A2P, so businesses utilizing long codes for their campaign messaging would see higher filtering by the carriers. However, carriers are now offering new long-code routes intended specifically for Application-to-Person 10-Digit Long Codes (A2P 10DLC), which improve deliverability and increase throughput. For businesses, this means you can keep the same local long code, but now function on an A2P-specific route without the increase in filtering.

Local long codes are best used for messaging from a local number that triggers a conversation or response from the user—for example, a delivery driver telling you that your food is on its way or a conversation with a business for tech support.

A2P 10DLC phone numbers, which are now required for any local long-code phone number within the U.S., are required to register their business profile and brand registration along with their campaign use cases. This registration builds trust with the carriers and ultimately with the consumers, which is the primary goal.

You can learn more about A2P 10DLC numbers here.

Toll-free numbers are 10-digit phone numbers (e.g., 800-234-5618) that may also be purchased through Twilio's API or Console and 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 up to 150 MPS with High Throughput Toll-Free. Messages sent from toll-free numbers can be filtered at the carriers' discretion, just like long codes.

Toll-free numbers provide your business with a universal brand identity and are best suited for support and sales messaging. Due to a lower volume of throughput and deliverability compared to short codes, marketing and notification-based messaging is not always an ideal use case for toll-free numbers.

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

Note: If you are seeing a higher number of filtered messages from your toll-free numbers, Twilio recommends that you complete the optional verification process. This will ensure that the carriers know who is specifically sending the messages and may result in lower filtering.

For additional information on all phone number types, visit the Twilio's 2021 Guide to Business Messaging Number Types.

The opt-ins and outs of messaging consumers

Because the goal of a compliant campaign is to only send communications that consumers or constituents 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. It is worth noting that these same requirements extend to other A2P messaging channels, such as WhatsApp, Facebook Messenger, and Google Business Messages.

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, it's important that opt-ins are contextual and timely. The goal is to ensure that you and the consumer are both clear about whether that consumer wants to receive the particular messages you intend to send.

Think of this in terms of campaigns: Consumers should be opting in for specific messages during a reasonable time period. For example, a shopper signing up for one holiday-specific promotion does not necessarily indicate an opt-in for the next one. Customer experience is affected when messages are sent for unrelated reasons and when messages are sent long after the recipient remembers opting in to receive them.

Under the TCPA, certain opt-ins—such as for automated SMS marketing messages—must be logged in writing, whether 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 or not your messages are promotional, 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 risks related to customer complaints, we recommend establishing a double opt-in. Once a consumer opts in, remind them that they signed up with their first message, then have them respond with their consent to begin the messaging campaign. While this isn't always necessary, it is an industry best practice.

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

In addition to "STOP" initiating a consumer's opt-out, businesses must also initiate a compliant response when consumers reply with the keyword "HELP" to any short code message, regardless of whether the recipient is subscribed to the program.

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, 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, asking the consumer to text a phone number 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.

Short code example

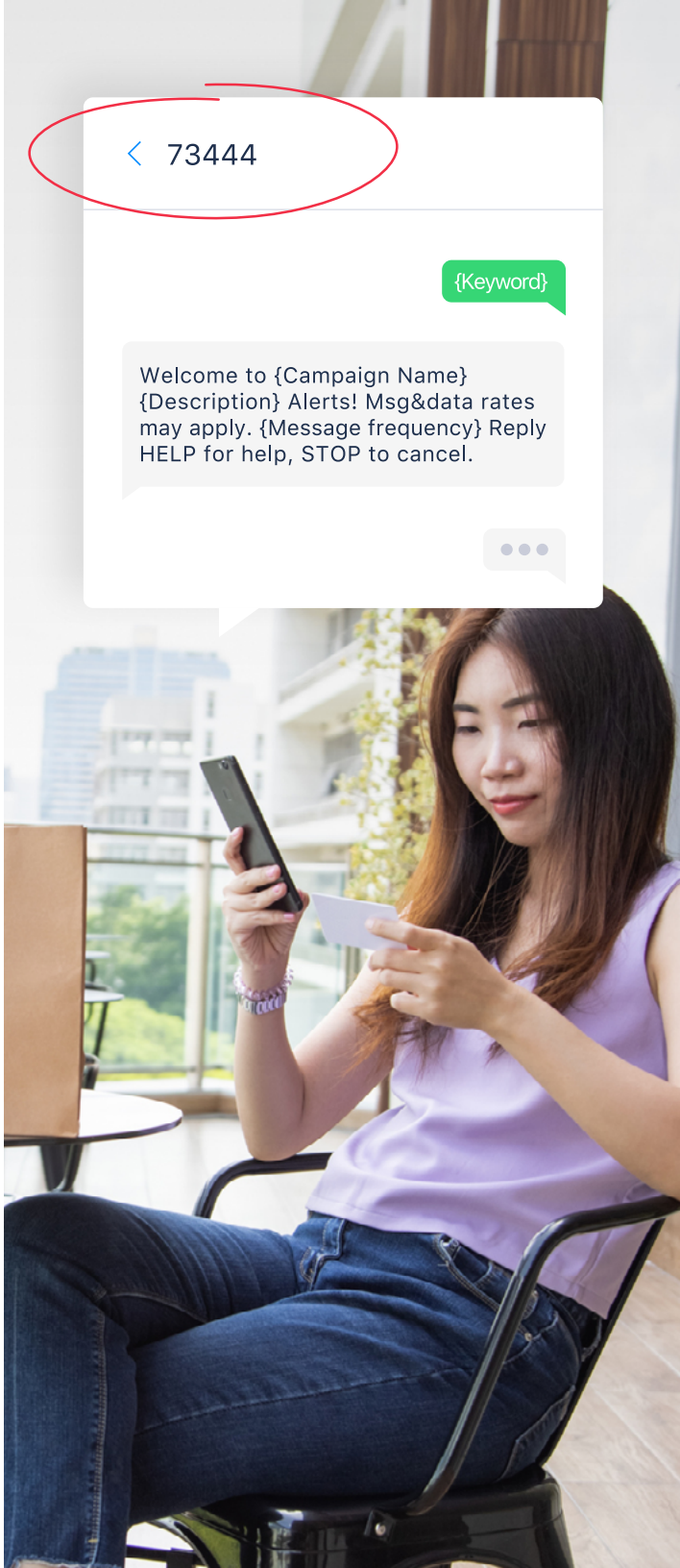
Recipient: {Keyword}

73444: 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:

Short code

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.

73444: Text YES to join {Campaign Name} {Description} Alerts. Msg&data rates may apply. {Message frequency} Reply HELP for help, STOP to cancel.

Recipient: YES

73444: 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.

Local long code

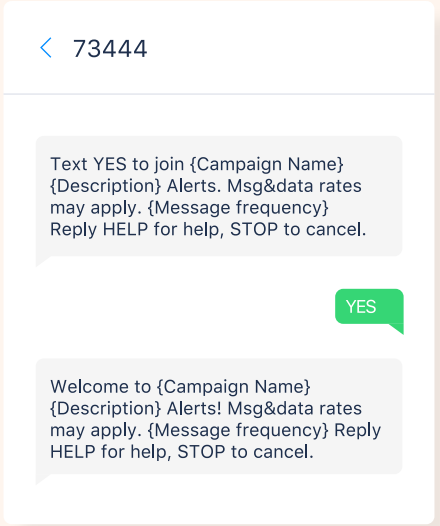
Recipient signs up for messaging with a customer service representative at a local business and receives a text message from a local 10-digit long code number asking to confirm the opt-in.

845-555-2352: Text YES to receive and send messages regarding {Campaign Name} {Description} Alerts. Msg&data rates may apply. {Message frequency} Reply HELP for help, STOP to cancel.

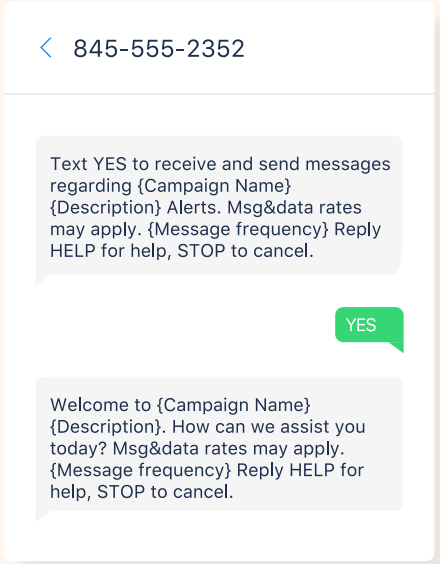
Recipient: YES

845-555-2352: Welcome to {Campaign Name} {Description}. How can we assist you today? Msg&data rates may apply. {Message frequency} Reply HELP for help, STOP to cancel.

Short code example



Long code example



IVR opt-in

There are a few types of opt-ins newer to 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 long hold times. The consumer has an option to "Press 1" to begin a messaging support conversation.

Short code 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.

> 73444: Text YES to join {Campaign Name} {Description} Alerts. Msg&data rates may apply. {Message frequency} Reply HELP for help, STOP to cancel.
>
> Recipient: YES
>
> 73444: Welcome to {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.

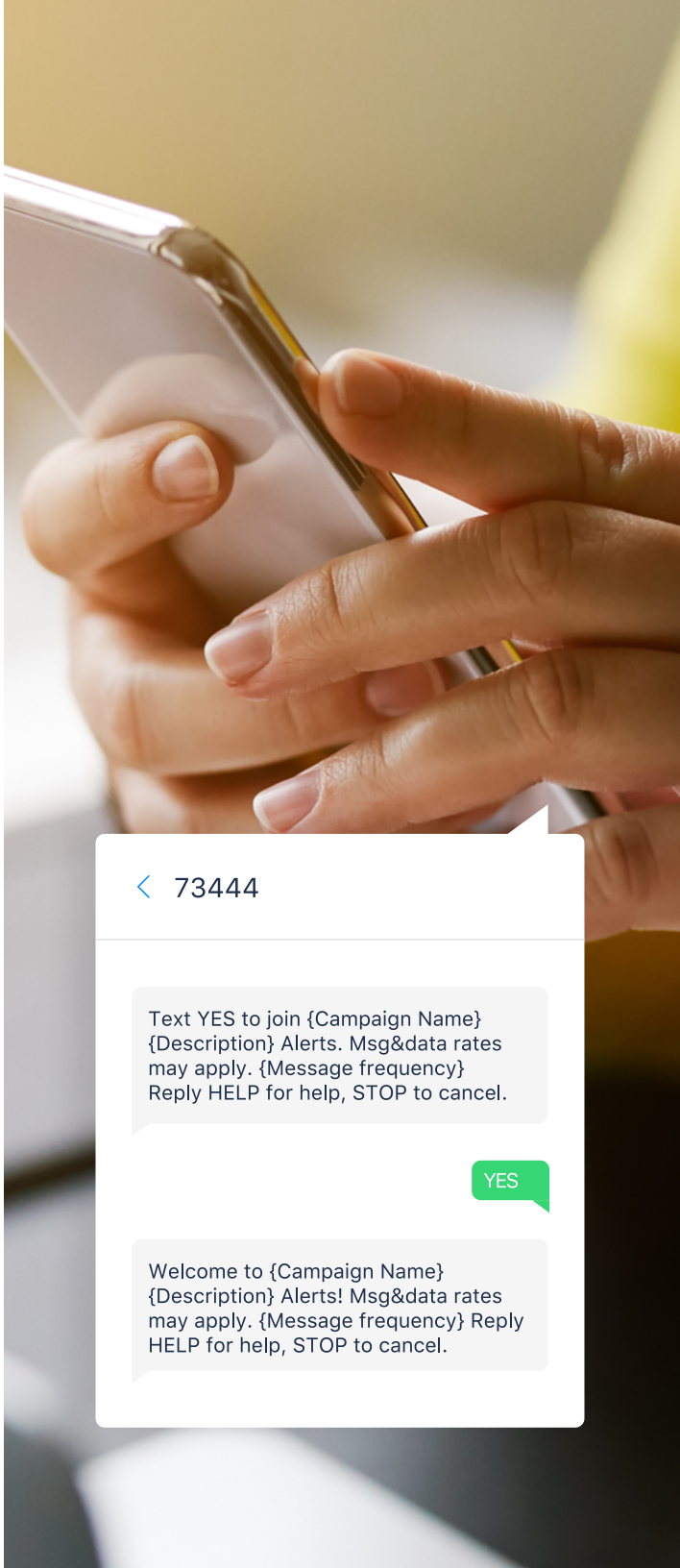
Point-of-sale (POS) opt-in

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

Short code example

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

> 73444: Text YES to join {Campaign Name} {Description} Alerts. Msg&data rates may apply. {Message frequency} Reply HELP for help, STOP to cancel.
>
> Recipient: YES
>
> 73444: Welcome to {Campaign Name} {Description} Alerts! Msg&data rates may apply. {Message frequency} Reply HELP for help, STOP to cancel.



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 under Additional Resources.

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 nonstandard keywords in addition to the default keywords.

For a more refined approach, Twilio offers Advanced Opt-Out, which gives businesses granular control over the end-to-end compliance experience for customers and users, along with customizing opt-out keywords and confirmation messages.

Long codes

For 10-digit phone numbers (A2P 10DLC and Toll-Free), Twilio handles opt-outs for the following replies: STOP, STOPALL, UNSUBSCRIBE, CANCEL, END, or QUIT. Any future messages will serve the error code 21610 and fail to send to consumers who have opted out. You can track delivery and opt-outs of SMS in real time using status callback URLs, or use the API to query your logs for messages that contain these opt-out keywords in the body, like STOP. Lastly, you can use

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 the recipient's request.

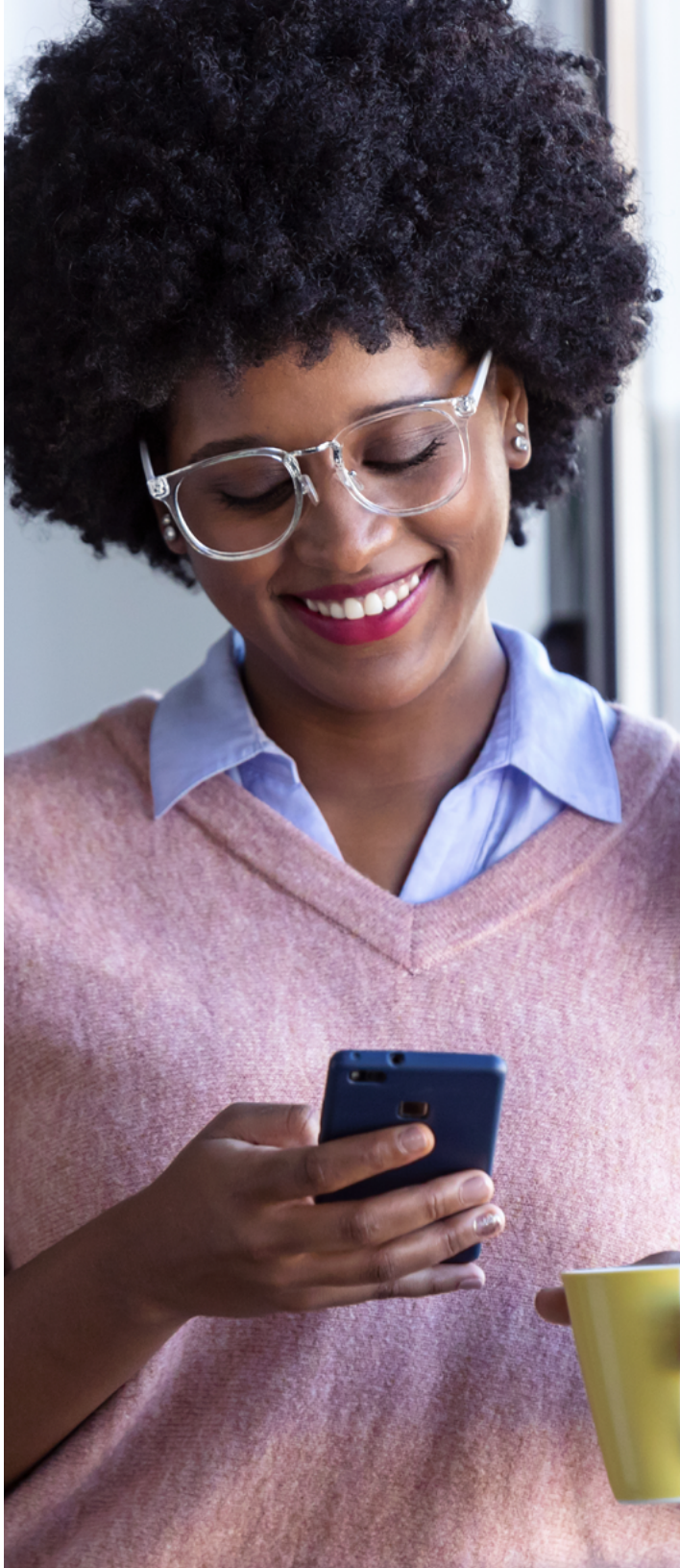
Users can always opt back in by replying START, YES, and UNSTOP (keywords are not case-sensitive).

Advanced Opt-Out for Messaging Services supports many of the intricacies of a customized compliance lifecycle for most businesses, and Twilio customers can manage these through their Console.

Short codes

By default, Twilio does not handle opt-outs for short code phone numbers on behalf of our customers. 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 who have opted out of receiving future messages to create a more branded opt-in/out experience, to 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 phone 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: by 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 their phone number is still the same.



Conclusion

A great messaging experience will delight your customers or supporters and is key to delivering strong 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 a potential 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 Book

CTIA Messaging Principles and Best Practices

Twilio Acceptable Use Policy

Twilio Messaging Policy

Forbidden Message Categories

Short Code Registry

A2P 10DLC Resources

Twilio SMS Guidelines by Country

Advanced Opt-Out Documentation

Managing SMS Between Your Users

Thanks for reading

If you would like to learn more about what Twilio can do for your business, please contact the Twilio sales team or give us a call at 844 814 4627.