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.

Revision #3
Created 2024-11-08 18:08:26 UTC by Vox Tandem Admin
Updated 2024-11-11 13:58:07 UTC by Vox Tandem Admin