



Must-Know Twilio Information

Text messaging gives businesses direct access to their customers, but that access comes with strict rules. Every business using a messaging platform connected to Twilio is responsible for ensuring that its messages are wanted, lawful, and consistent with Twilio and wireless-carrier requirements.

Failure to follow these requirements can cause messages to be filtered, a campaign or phone number to be suspended, or messaging access to be terminated.

1. Only text people who have given permission

You must obtain the recipient's consent before sending any text message.

- Consent must be freely given, clear, and specific to the business sending the messages.
- The person must understand what types of messages they are agreeing to receive.
- Promotional or marketing messages require prior express written consent.
- Consent cannot be purchased, sold, rented, transferred, or shared between businesses.
- You must keep records showing when and how each person opted in.
- A customer texting your business first allows you to respond to that particular conversation. It does not automatically give permission to send ongoing marketing messages.

Do not upload purchased lists, shared lists, scraped phone numbers, or contacts who have not specifically agreed to receive messages from that business.

2. Clearly identify the business

Recipients should never have to guess who sent a message. Twilio requires each message to clearly identify the business that obtained the recipient's consent, except for follow-up messages within an ongoing conversation.

Include the business name in every campaign message.

Example:

Riverside Coffee: Get 20% off your next order this Friday.

3. Make opting out easy

The first message sent to a recipient must include clear opt-out instructions, such as "Reply STOP to unsubscribe." Recipients must be able to opt out in one simple step.

When someone replies STOP or uses another recognized opt-out keyword, the platform automatically processes the request, marks the recipient as opted out, and prevents additional campaign messages from being sent to that number. No manual removal is required.

Twilio recognizes standard English opt-out terms including STOP, STOPALL, UNSUBSCRIBE, OPTOUT, CANCEL, END, REVOKE, and QUIT.

The platform automatically adds "Reply STOP to opt out" to campaign messages.

When someone replies STOP or uses another recognized opt-out keyword, the platform automatically processes the request, marks the recipient as opted out, and prevents additional campaign messages from being sent to that number. No manual removal is required.

4. Follow quiet hours

Non-essential texts must be sent according to the recipient's local time—not the sender's time zone.

Twilio identifies the federal TCPA quiet-hours window as 9:00 p.m. through 8:00 a.m. in the recipient's local time zone. Some states impose stricter requirements.

As a practical standard, schedule marketing campaigns between 9:00 a.m. and 8:00 p.m. in the recipient's local time zone. This narrower window is intended to reduce the chance of sending during restricted hours, but businesses remain responsible for any additional state or local requirements that apply to their recipients.

5. Do not send SHAFT content

"SHAFT" refers to five categories of content that wireless carriers treat as prohibited or highly restricted for A2P messaging:

- S — Sex: adult content, pornography, nudity, sex-related products, or sexual services
- H — Hate: hate speech, threats, content that promotes violence, or similarly abusive content
- A — Alcohol: messages that advertise, promote, or refer to alcoholic products
- F — Firearms: firearms, ammunition, weapons, or related sales and promotions
- T — Tobacco: cigarettes, cigars, vaping products, nicotine products, or related sales and promotions

Twilio's A2P 10DLC guidance also identifies marijuana references as a content violation. This can apply even where cannabis is legal under state law.

Do not attempt to avoid filters by intentionally misspelling prohibited words, using symbols in place of letters, or spreading similar messages across multiple phone numbers. Twilio expressly prohibits attempts to evade its detection and prevention systems.

6. Other prohibited or high-risk messaging

Businesses must not use the platform to send or promote:

- Unsolicited bulk messages or spam
- Illegal goods, services, or activities
- Controlled substances
- Phishing or deceptive requests for personal information
- Fraudulent or counterfeit products or services
- Promotional gambling or betting
- Affiliate marketing that relies on shared or transferred opt-ins

- Illegal sweepstakes
- Simulated phishing or other security-testing messages

Campaign traffic must also match the use case registered for that business. A campaign may be suspended when its actual messages do not match its approved registration.

7. Before sending a campaign

Confirm all of the following:

- Every recipient specifically opted in to messages from this business.
- The business has retained proof of consent.
- The message identifies the business.
- The content matches the purpose for which the recipient opted in.
- The message contains no prohibited or misleading content.
- The campaign is scheduled for an appropriate time in each recipient's local time zone.
- Opt-out instructions are included.

When in doubt about a business type, promotion, or message, do not send the campaign until its eligibility has been confirmed.

Sources

- [Twilio Messaging Policy](#) – consent, sender identification, opt-outs, prohibited actions, and unwanted messaging
- [Twilio Compliance Toolkit](#) – federal and state quiet-hours enforcement
- [Twilio A2P 10DLC Campaign Troubleshooting](#) – SHAFT violations, prohibited campaign content, and campaign suspensions
- [Twilio Advanced Opt-Out](#) – recognized opt-out keywords and blocking after opt-out

This article provides general operational guidance and is not legal advice. Businesses are responsible for complying with all laws and rules that apply to their messaging.