Text Message Lawsuits on the Rise: Top 10 Steps Businesses Should Consider For TCPA Compliance

Insights
1.14.26

We have started to see a shift in consumer privacy litigation as plaintiffs' attorneys and state regulators are increasingly targeting the common business practice of sending text messages. While texting carries with it great business benefits, it also comes with a high risk of class actions and significant statutory damages if not done properly. And the trend toward state-level regulation is likely to continue, making it essential to stay abreast of legislative, regulatory, and judicial developments. For businesses operating national campaigns, this combination of state-by-state statutory differences and evolving legal standards creates a complex and risky compliance environment. What are the top 10 things your business needs to do to implement safeguards to avoid costly litigation?

The New Wave: Plaintiffs Targeting Unwanted Text Messages

The Telephone Consumer Protection Act (TCPA) was enacted in 1991 in response to unwanted telemarketing calls and the use of autodialing technology. But it's now being used as a weapon in texting litigation thanks to the proliferation of mobile devices, evolving marketing practices, significant statutory damages available under the statute, and the ability to file class action suits.

The most common fact patterns involving text message disputes include:

- **Lack of Consent:** Courts addressing alleged lack of consent focus on whether consent to receive the texts was explicitly provided. A consumer that simply provides a phone number to a business has not provided sufficient consent for marketing text messages, for example. It is the company's burden to prove that something more happened to demonstrate proper consent, and this is almost always impossible to demonstrate without adequate records.
- **Mistaken Opt-Ins and Scope of Consent:** A common fact pattern involves mistaken opt-ins, where a consumer may have provided consent for one type of communication, but not for marketing messages. A related fact pattern occurs where a business allegedly obtained consent through an ambiguous or misleading way. Issues also arise where a consumer mistakenly (or purposefully) provides an incorrect phone number and another person starts receiving inadvertent messages. Courts have consistently found that consent must be transaction-specific in order to satisfy the law and cannot be inferred from unrelated communications.

- **The Autodialer Debate:** Federal law restricts calls and texts made with an "autodialer" (or ATDS, an automatic telephone dialing system) unless the caller has the appropriate level of prior consent. However, the lack of definitive regulatory guidance in this area has left courts to resolve the issue on a case-by-case basis. This has contributed to the volume and unpredictability of TCPA litigation.
- **Incorrect and Reassigned Phone Numbers:** Generally, courts have held that liability attaches when a business sends a message to an actual recipient, regardless of whether they were the intended recipient. The broad interpretation increases risk of businesses, which may be liable for messages sent to numbers that have been reassigned without their knowledge.

Top 10 Steps Companies Can Take To Mitigate Their Risk

1. Obtain clear, conspicuous, and specific consent. Language regarding consent must be clear to a reasonable consumer and separate from other disclosures or advertisement copy. Bundled consent (where consent for telemarketing is bundled with other agreements, like signing up for a newsletter or accepting terms of service), or ambiguous consent is insufficient and ripe for disputes.

2. Ensure electronic consent is E-SIGN complaint. Electronic signatures, including checking a box on a website, are valid if they comply with the E-SIGN Act and the consumer affirmatively indicates consent.

3. Do not use pre-checked boxes and opt-out mechanisms. A consumer must take an affirmative step to indicate consent. Consent obtained through pre-checked boxes or opt-out mechanisms, wherein a consumer must uncheck a box to avoid consent, is insufficient.

4. Consent must be seller specific. Unless consent specifically identifies all entities that can contact a consumer, consent cannot be transferred from one entity to another.

5. The burden of proof is on the defendant. A defendant must prove they obtained valid consent.

6. Review and implement compliance policies: Review the most recent TCPA rules and changes to see how they could affect business. Using legal counsel familiar with TCPA compliance is an excellent way to ensure you are compliant with the law.

7. Use a consent management system: Consent management systems can help track and store records of consumer consent. It is important to document consent and ensure it is readily available in the event of litigation or regulatory inquiry.

8. Scrub your call list against the Do-Not-Call list: Companies should automate their process of scrubbing call lists against the DNC, which can reduce or avoid the risk of accidental non-compliance.

9. Have an easy opt-out mechanism: Providing a user-friendly opt-out option is important in every communication with a consumer. These requests should be processed in real time and should be updated automatically to avoid accidental violations.

10. Provide employee training: You should train employees involved in customer communications, marketing, and compliance on TCPA compliance regularly. Ensuring that employees obtain clear consent, follow DNC rules, and facilitate easy opt-out mechanisms is critical to mitigate legal risks.

Conclusion

For support, feel free to reach out to your Fisher Phillips attorney, the authors of this Insight, or another member of our Consumer Privacy Team or Privacy and Cyber team. We'll continue to monitor TCPA litigation and provide updates as warranted, so make sure you are signed up for Fisher Phillips' Insight service to receive the latest news directly in your inbox.

Related People

Catherine M. Contino
Associate
610.230.6109
Email

Brett P. Owens
Partner
813.769.7512
Email

Service Focus

Privacy and Cyber

Consumer Privacy Team

Trending

U.S. Privacy Hub