STATFLO

Text Message Compliance:
How Statflo Can Help Organizations Comply With SMS Regulations

Table of Contents

Introduction

At the present time, many organizations are implementing innovative customer outreach platforms in order to make the digital transition this era calls for. In general, customer engagement platforms assist companies in managing, analyzing, and optimizing the customer journey for the most ROI. These platforms accomplish this by automatically sending personalized messages to customers on multiple platforms and devices. Despite the great benefits that businesses may get from adopting these technologies, it is important that they are aware of the laws and regulations that dictate how customers can be contacted and how to manage their data. Interestingly, customer outreach platforms have existed for a long time, but have primarily emphasized email communications over SMS.

The use of SMS for business is gaining more popularity as new research has found that **98%** of customers will read incoming messages, **86%** of businesses report that texting generates engagement 6 to 8 times higher than email, and **75%** of customers will redeem offers sent via SMS. While SMS can be effectively included as part of a marketing strategy, brands must adhere to regulatory requirements and practice standard text messaging etiquette to keep their relationships with customers beneficial.

SMS marketing messages are governed by regulations such as the U.S. **Telephone Consumer Protection Act of 1991** (TCPA) and the **Canadian Anti-Spam Law** (CASL), which have quite stringent requirements. Before sending messages to customers, businesses must disclose their practices clearly and conspicuously and obtain the recipient's explicit consent to receive them. Furthermore, they should check for the legal age of consent based on where the recipient is located.

The purpose of this whitepaper is to describe SMS regulations and compliance, a topic Statflo takes very seriously. Statflo understands the legal, financial and overall business risks companies may face if they don't follow these laws and regulations correctly, and have created a software that ensures businesses have one less thing to worry about when messaging customers.

Upon further review of this document, you will;

- Acquire a deeper understanding of what SMS regulations are
- Identify how they apply to business text messaging
- Become familiar with compliance regulations that Statflo platform covers
- Gain an understanding of who they impact, and how they may affect a business
- Learn about SMS etiquette: consent, opt-in/opt-out, when to contact customers, etc.
- Gain awareness of the consequences of failing to comply
- Learn how Statflo helps companies remain compliant with SMS regulations

What are SMS Regulations?

It is important to remember that customer consent is the most important aspect of complying with SMS laws. Nevertheless, consent is only one aspect of the subject; protecting people's information is also an important consideration. SMS regulations are not the same in every country. In many countries, including the United States, the United Kingdom, Canada, Australia, and Member States of the European Union, texting customers is regulated differently. Though one thing all these regions have in common; a customer's written consent is required before sending any kind of communication.

Obtaining consent is also necessary for customers who have previously transacted with the organization and whose contact information is still on file with the organization. It is crucial that companies utilizing SMS in their marketing strategy adhere to regulatory requirements and follow text messaging best practices to maintain customer relationships. When contacting customers, text spam laws should also be considered, however, text marketing rules continue to evolve and will undergo significant changes throughout the years. Ensuring that you keep abreast of SMS marketing laws is highly crucial.

Federal and local governments around the world regulate the use of business text messages. It is imperative that businesses be aware of regulatory requirements wherever they operate and where their customers are located. Because of this, text message compliance can be challenging for organizations who have never dealt with it before. Businesses must also clearly disclose their practices and obtain the recipient's express written consent to receive text messages before sending messages.

Practicing SMS compliance has a lot of intricacies to it but it is still possible to navigate the world of business text messaging without a significant amount of worry if you have a firm understanding and strategy in place.

Most of the text messaging laws described in this white paper support the same general principles - such as prior consent and the ability to unsubscribe - but there are still subtle differences between them. Understanding these differences can help you adjust your SMS marketing strategies accordingly for different geographical areas and/or industries. So with that in mind, let us take a closer look at each.

SMS Regulations Statflo Complies With

TCPA

A major objective of the **TCPA** (an American regulation) is to prevent repetitive, irrelevant, or excessively intrusive telephone calls. The TCPA applies to all forms of outbound telephone contact, such as autodialed and manual telephone calls, faxes, voice messages (organic and automatic), text messages, and automatic dialing systems.

The TCPA created the **national do-not-call list** (DNC), and the Federal Communications Commission (FCC) is responsible for implementing the TCPA through rules and regulations prohibiting companies from contacting customers who are listed on this registry. It is essential that at least one of the following conditions be present for communicating with people on this list: either there must be an established business relationship, some sort of inquiry, or written consent from the individual.

TCPA General Guidelines Checklist for Text Message Communications;

- In order to initiate a marketing call or text, the recipient must first provide prior express written consent (PEWC).
- Do not contact residents prior to 8 a.m. or after 9 p.m. local time.
- You should not text or call anyone listed on the National Do Not Call Registry.
- Please ensure that the recipient has the option to opt-out and have their number added to the **DNC** list if using a prerecorded message.
- You should maintain a “Do Not Contact” list for your business contacts and honor requests for five years
- Whenever you contact a customer, provide them with your name, the name of your company, and a phone number or email address where they can reach you.
- It is not advisable to purchase lists of phone numbers with contacts who have not opted in.
- Stay up to date with regulatory updates by checking regularly.

CASL

Canada Anti-Spam Legislation (CASL) went into effect in 2014. It is similar to TCPA in that it applies to telemarketing and protects Canadians from spam calls and text messages. As a result of Canada's anti-spam legislation (CASL), consumers and businesses are protected from the misuse of digital technology, including spam and other electronic threats. Furthermore, it is designed to help businesses stay competitive in a global, digital marketplace.

- Under CASL, there are two types of consent - implied and express. In implied consent, a company can contact someone either if they disclose their contact information publicly or if they provide it through an existing business relationship. Express consent is when a person explicitly gives a business the permission (in writing, through opt-in, or digitally) to send promotional messages
- Implied consent has an expiration date of two years after which companies can no longer legally send commercial electronic messages to people. Express consent is valid till the person withdraws it
- CASL requires businesses to send their identification information as well as a link to unsubscribe from the communication and opt-out from the promotion list within the text message.

GDPR

In general, the General Data Protection Regulation (GDPR) is a regulation enacted by the European Union (EU). It applies to any country entering into business with or using personal data belonging to EU citizens. The regulation relates both to data security and to marketing communications.

GDPR requires companies to obtain permission prior to sending marketing messages to individuals, similar to CASL and TCPA. The GDPR specifies **stringent provisions about data protection** in addition to anti-spam rules, such as implementing security measures around data collection, reporting any security breaches to customers within 72 hours, and providing customers with the ability to access their data.

PIPEDA

PIPEDA deals with private sector organizations or businesses that are engaged in commercial activities. Pipeda defines these activities as follows:

"commercial activity means any particular transaction, act or conduct or any regular course of conduct that is of a commercial character, including the selling, bartering or leasing of donors, membership or other fundraising lists. (activité commerciale)"

In brief, here is an overview of the PIPEDA principles:

- Personal information under your control must be protected. An individual who is responsible for PIPEDA compliance must be appointed (often referred to as the "Privacy Officer").
- At the time of collection or before, you must identify the purposes for which you are collecting personal information.
- It is your responsibility to obtain consent when collecting, using, or disclosing personal information where appropriate.
- If you are collecting personal information for a specific purpose, you may only collect that amount of information that is necessary for that purpose.
- Personal information should only be used or shared for the purposes for which it is collected (unless you have the consent of the individual or are legally required to use or share the information for another purpose).
- Personal information should not be retained for longer than is necessary.
- Personal information must be protected using appropriate security measures.
- Each individual has the right to access and correct his or her personal information.
- Individuals must have the ability to challenge your compliance with PIPEDA by submitting a complaint.

The Statflo messaging platform is used by financial institutions who often handle a significant amount of customer information. It can be quite cumbersome for companies to process all this information, so working with software that includes a built-in PIPEDA compliance checklist solves a lot of problems that may arise from mishandling of data.

CTIA

As a trade organization in the United States, the Cellular Telecommunications Industry Association (CTIA) represents the wireless industry. Contrary to TCPA, CASL, or GDPR, it is not a legally binding statute - meaning carriers and dealers cannot be sued if they do not follow the CTIA rules. If a telecom dealer violates CTIA's guidelines, the mobile carrier may suspend the telecom dealer's access to its customers until the issue has been resolved.

SOC2 Type II

SOC 2 reports are designed to provide assurance to clients, management, and users of service organizations regarding the suitability and effectiveness of their security, availability, processing integrity, confidentiality, and privacy controls. Access to the reports is usually restricted to existing and prospective clients only. Unlike other regulations, **SOC 2** provides greater assurance than simply saying you are compliant as it is an independent audit conducted by a third-party accounting firm.

SOC audits and reports fall into two categories:

- Type 1 - a review and report conducted on a specific date.
- Type 2 - an audit that is conducted over a particular period, usually a minimum of six months.

SOC 2 audit reports include the following information:

- An opinion letter.
- Management assertion.
- Detailed explanation of a product or service.
- Information about the selected trust service categories.
- The results of the tests and the controls.
- Other optional information.

The service organization is also evaluated on whether it complies with the AICPA TSC. It is not surprising that there is a greater emphasis on information security today given the proliferation of data breaches and hacks that occur. Reports from SOC 2 are generally used to assure users, organizations, and stakeholders that a particular service is secure. Additionally, SOC 2s can include operational criteria related to availability, confidentiality, processing integrity, and privacy.

While SOC 2 compliance is not a requirement for SaaS and cloud computing vendors, its importance cannot be overstated when it comes to protecting your data.

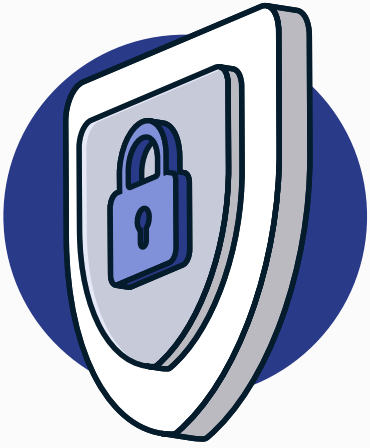
"These certifications require abiding by ongoing internal processes that fall in line with stringent compliance measures. This extra step of successfully completing the voluntary audits shows that we have not only designed systems and controls for data protection, but we also follow the processes continuously - something our customers find comfort in."

For a second year in a row, Statflo recently completed the Service Organization Control (SOC) 2 Type II audit. As a result of this certification, Statflo has reinforced the operational efficiency and integrity of its systems, as well as solidifying its position as a **privacy-conscious software.**

The **American Institute of Certified Public Accountants** (AICPA) designed and developed SOC 2 Type II, a voluntary certification applicable to all SaaS companies that store customer data in the cloud. Following the successful completion of this technical audit, Statflo has established and continues to maintain enterprise-grade security procedures pertaining to customer data.

"At Statflo, we take data security and privacy of customer information very seriously. The SOC 2 Type II and PIPEDA audits reiterate our commitment towards exceeding the privacy and security requirements of all our clients," says Ian Gervais, Vice President of Product at Statflo.

In addition to SOC 2 Type II, Statflo has also successfully passed the PIPEDA audit (mentioned above), which is the Canadian law that protects personal information. In some cases you can't enter a particular market without a SOC 2. For example, if you are selling to financial institutions, they will almost certainly require a Type II SOC 2 report.



Impact of SMS regulations on SMS marketing

Although there are no rules prohibiting an individual from texting someone else - even without their permission -- the same can't be said for business-to-consumer messaging. In other words, a person's text message inbox should be considered to be an item of personal property. Therefore marketing messages - basically considered to be solicitations- when sent to an individual without their consent violates their privacy. The act of doing so may be considered harassment so if you wish to send SMS marketing messages, all the regulations mentioned above have clearly stated how to go about it and that consumers must consent to contacting them.

Early on in the development of SMS marketing, there were no safeguards in place to prevent businesses from simply purchasing contact information and potentially spamming customers
Consequently, several agencies were formed to protect the privacy of consumers and ensure that businesses behave appropriately when sending SMS messages. By following SMS compliance requirements, you can ensure that your business is protected against lawsuits.

In 2020, for example, the **FCC proposed a $225 million fine** against a group of individuals for making robocalls to consumers listed on the federal Do Not Call List and for contacting wireless consumers without consent. To date, this has been the highest fine under the FCC for violating the TCPA.

Typically as a business, you should work with your legal team before you begin building your SMS marketing audience to ensure that the program you develop is legally compliant. It is extremely important to understand that SMS marketing constitutes a type of **permission-based marketing**.

The customer should only be able to receive your messages if they have provided your organization with written consent which usually happens through an online submission. If you wish to grow your contact list as a business, the message you advertise must expressly indicate that you will text them in the future. When you send a text message to a customer without their explicit consent, you are spamming them, which is against compliance regulations. Opting in also requires people to check a box that outlines the program's terms and conditions.

It is important that you ensure all of your contacts have opted in to receiving messages from your company prior to using texting softwares like **Statflo**. You should also maintain your contact lists regularly. All sms marketing messages sent out to customers must also include a link or shortcode like 'STOP' that enables them to opt out anytime from receiving messages. Retailers should have a robust and automated workflow in place to **manage opt-outs and DNCs** so that they don't accidentally contact those who unsubscribed.

How Statflo Help Businesses Stay Compliant with SMS Regulations

Statflo, at the time this whitepaper was published, serves a wide spectrum of industries, including financial services, telecommunications, and insurance. Although each of these industries is unique in its operations and way of conducting business, they are all subject to the same business texting regulations and other general texting etiquettes. Statflo has succeeded in focusing specifically on the legal differences for SMS marketing laws and regulations that are unique to these industries and created a business texting platform that helps to keep companies compliant when sending marketing messages to customers.

Among the things that make Statflo unique is that it is currently the only fully compliant SMS platform available on the market. Businesses that have integrated this software into their customer relationship management systems like Salesforce, for example have one less thing to worry about, since failure to comply with these rules has grave consequences.

The following attributes also contribute to the superiority of the Statflo app over other messaging softwares:

- Statflo contains a built-in smart filtering feature that ensures inappropriate language and content are flagged and blocked from being sent or received.
- We offer coaching tips to ensure that your staff understand why a word or phrase is flagged and ensure it is corrected before the message is sent.
- We ensure that you are adhering to industry standards and local/national regulations.
- Our DNC management tool helps you handle opt-outs automatically for all available communication channels.
- We distinguish ourselves from similar softwares like ZipWhip by offering a dedicated customer success manager for your account.

The use of text messaging as a channel for customer outreach is clearly not without its own complexities. Compliance with legal requirements and data security are among the most important considerations for retailers when implementing text-based marketing outreach programs. In light of the ambiguous nature of certain statutes, communicating with customers without following proper protocol would be similar to walking on thin ice.

To prevent text messages from being interpreted as spam, Statflo has built-in safeguards that can flag salesy language and words that could be considered offensive, spammy, or discriminatory. Some words, such as 'free', 'urgent', 'giveaway', and 'contest', trigger spam filters and cause the recipient to block the sender from sending further messages. Businesses should only send text messages that add value to the recipient instead of sending a direct sales pitch to avoid spam blockers.

Being compliant as a business is complex and involves many moving parts and rules that you should be aware of as a business not to violate. One way to accomplish this goal is by establishing a compliance team but even better, consider using software programs with an intelligent filtering system that can automate the whole process.

To learn more about Statflo
[Book a Demo]

Find out more

statflo.com