gryphon.ai

The Risks of TCPA and DNC Violations and How to Prevent Fines

Learn about the most common violations, where your enterprise is most at risk, and the steps you can take to avoid damaging fines and lawsuits.

The Risks of TCPA and DNC Violations and How to Prevent Fines and Lawsuits

In today's digital age, telemarketing remains a powerful tool to help reach new customers. But navigating the complex regulation landscape can be difficult and the risks of violating telemarketing laws and legislation can cost your organization more than just money.

This guide dives into common types of TCPA and DNC violations, the risks associated with violating those regulations and how you can prevent them within your organization to stay compliant and avoid costly penalties.

Compliance Regulations

Understanding the risks of violating the Telephone Consumer Protection Act (TCPA) and Do Not Call (DNC) regulations starts with understanding the regulations themselves.

The TCPA was created to protect consumers from unwanted telephone marketing calls by restricting the use of an automated telephone dialing system (ATDS), often referred to as an autodialer, and maintaining and adhering to DNC lists.

Like the federal TCPA law, many states are passing their own telemarketing legislation. Some of the differences in the laws include call frequency limits, consent requirements, the definition of an autodialer and telemarketing call, as well as minimum and maximum penalties per incident.

The National Do Not Call Registry is a database maintained by the United States federal government, listing the telephone numbers of individuals and families who have requested that telemarketers not contact them.

Under the TCPA, it is prohibited to contact someone who has registered their phone number on the DNC. In addition to the National DNC registry, 11 states operate their own DNC lists: Colorado, Florida, Indiana, Louisiana, Massachusetts, Missouri, Oklahoma, Pennsylvania, Tennessee, Texas, and Wyoming.

It's important to note that organizations may also have internal DNC lists that also must be honored and maintained to prevent TCPA violations.

**This guide is intended to provide a general overview of a topic and is not legal advice.*

Common types of TCPA and Do Not Call violations

Unauthorized pre-recorded voice messages (robocalls)

Unauthorized pre-recorded voice messages, otherwise known as robocalls, are unlawful under the TCPA, unless the caller has received express prior written consent to contact the consumer.

Unsolicited text messages

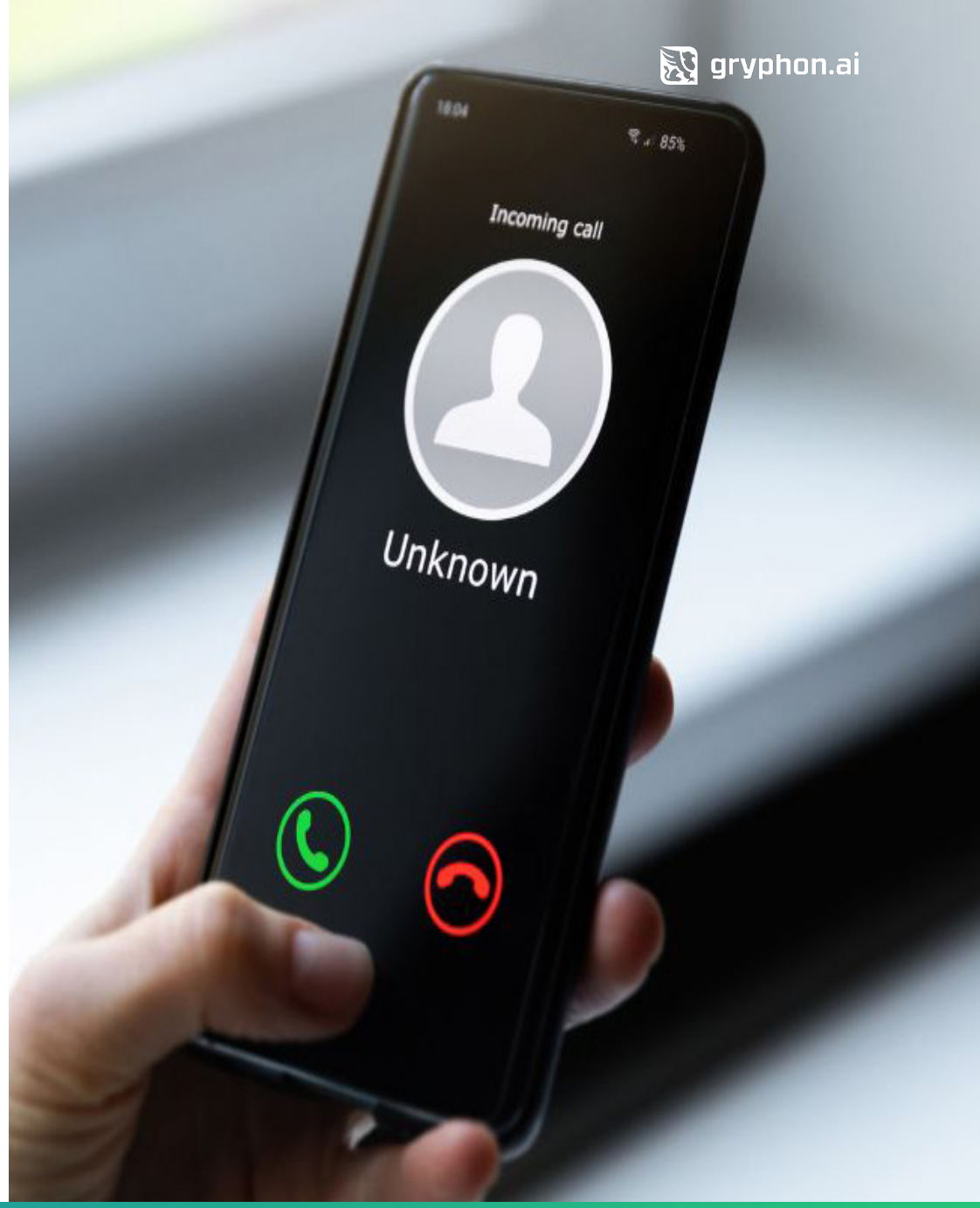
Unsolicited text messages are unlawful under the TCPA. The TCPA requires express written consent before contacting someone via SMS or text message.

Autodialed calls to cell phones

It is not permitted to contact someone on their wireless device using an ATDS. Only calls made to residential lines are permitted while using an ATDS or the system with a capacity to be an ATDS, unless the caller has received express prior written consent to contact the consumer.

Malicious caller ID practices (spoofing)

Misleading caller ID (often referred to as spoofing) is when the caller's name or business does not match the telephone number. It is prohibited display of false or misleading caller ID (spoofing) with the intent to defraud, cause harm, or wrongfully obtain something of value.



Common types of TCPA and Do Not Call violations (continued)

Do Not Call violations

Under the TCPA, it is prohibited to contact someone who has registered their phone number on the DNC. When you contact someone on the national, state, or internal DNC list, you are at risk of getting fined.

There are a few exceptions to Do Not Call violations (also known as "DNC violations"). If you have express written consent to contact someone, if you have an established business relationship, or if their state/internal-level DNC has expired then you may be able to contact them without penalty.

The National Do Not Call registry does not expire. Once you register your phone number on the National DNC, you never need to re-register it. State and internal DNCs, however, may have an expiration date. If the consumer you are trying to contact is on a state or internal-level DNC, they may be okay to contact after a period of time (depending on where they live/the internal DNC policy).

Established business relationships (EBR) are also a contact exemption. There are two types of EBRs: inquiry and past transaction.

An inquiry EBR happens when a consumer makes an inquiry about an organization's goods or services. In those cases, the company is permitted to contact the consumer for up to 3 months from the date of inquiry or application.

A past transaction EBR occurs when a company establishes a business relationship with a consumer based on the consumer's last date of purchase, delivery, or payment, and may then call them for up to 18 months after that last transaction. The rules and timelines of EBRs can vary by state/region, so be sure to understand the different nuances of where you are calling to avoid fines.

Express written consent is also an exemption. Regardless of if the contact is on a DNC list, if they give your organization express written permission to be contacted, you may contact them without being penalized.

It is important to note that while there are federal Telephone Consumer Protection Act and Do Not Call Regulations, many states have adopted their own guidelines. If you are calling any consumer for marketing or collections purposes, you need to ensure compliance with both federal and individual state regulations.

gryphon.ai

Risks of violating TCPA and DNC compliance regulations

There are multiple consequences of violating TCPA compliance regulations, ranging from monetary fines to damaged reputation.

Fines of $500 to $1500 per violation/call

The TCPA has a fine of $500 per violation/call if the caller unknowingly violates the TCPA and $1500 per violation/call if it proven that the caller willingly and knowingly violated any restrictions.

This may not sound like a lot, but these fines add up quickly if your organization is found to have made more than 1 unlawful call.

Civil lawsuits

In addition to monetary fines under the TCPA, civil lawsuits may arise from Do Not Call violations. A civil lawsuit occurs when an individual holds the responsible party accountable for financial and emotional losses that resulted from personal injury. Civil lawsuits seek financial compensation only, making them popular amongst TCPA cases.

While the fines for violating the TCPA can cost up to $500 or $1500 depending on the violation, there is no cap on statutory damages under the TCPA so thousands of dollars of violations can end up resulting in millions of dollars' worth of penalties.

TCPA and DNC violation penalties

Telephone Consumer Protection Act (TCPA)

- Up to a $500 fine per violation/call
- Up to a $1,500 fine per violation/call for willful violations
- There is no cap on statutory damages so thousands of violations can result in millions of dollars in penalties

Do Not Call (DNC)

- $43K+ at the federal level
- Up to $25K fines in select states

Risks of violating TCPA and DNC compliance regulations (continued)

Class action lawsuits

A class action lawsuit is a type of civil lawsuit in which charges against a company or individual are brought forth by several plaintiffs.

Class action lawsuits resulting from TCPA violations are among the most common types of class action lawsuits because TCPA violations have the largest payout in the history of American class action lawsuits. This is why understanding TCPA compliance is so critical to the success of your business.

Damaged brand and reputation

When businesses violate the TCPA, their brand and reputation are also affected negatively. The amount of money spent on fines and legal fees is nothing compared to the damage of a poor brand reputation.

The fines and lawsuits can be paid, but your brand reputation will suffer long after it becomes known that you violated the TCPA.

Reduced shareholder value

In addition to fines, lawsuits, and brand damage, violating TCPA compliance regulations may also result in reduced shareholder value.

Shareholder value is the value delivered by a company to investors who own shares in the company. When companies get hit with costly fines and lawsuits, the value of the company decreases, therefore reducing shareholder value as well.

This can result in substantial financial losses for investors, reduced ability to raise capital, and more.

Loss of consumer trust

Loss of consumer trust is another massive consequence of violating TCPA compliance laws. When you violate a consumer's privacy or do not honor their contact preferences by sending unsolicited messages or making unwanted calls, they are likely to lose trust in your business.

When consumers lose trust that you can operate your business ethically, they may never purchase your products or services again. Can your business afford to lose consumer trust?

How you can prevent TCPA and DNC violations

DNC and TCPA compliance should be top of mind for every organization performing telemarketing outreach. To safeguard your organization against the effects of violating TCPA regulations, follow these best practices.

Obtain proper consent

It is imperative that organizations obtain proper consent before contacting consumers. This is one of the main regulations under the TCPA, and the backbone of remaining compliant. Obtaining proper consent ensures your organization is complying with federal regulations, protecting consumer privacy, enhancing customer relationships, and mitigating risks.

Maintain and honor Do Not Call lists

Another best practice to safeguard your organization from TCPA violations is to maintain and honor Do Not Call lists. To avoid violating DNC regulations, it is important to avoid calling consumers who are on the federal, state or an internal DNC list. Companies that illegally call numbers on the national do not call registry can currently be fined up to $50,120 per call.

Keep records of consent

Not only is obtaining proper consent important, but keeping records of consent is equally important. In the case of an audit, you want to be sure you can provide the proper documentation needed. Failure to obtain clear and documented consent from consumers can lead to hefty fines and penalties.

In most instances, expressed written permission (consent) does not expire. Once a consumer opts-in to receive text messages, organizations are permitted to contact them until the organization receives an opt-out notice or consent is revoked. However, this rule can vary by state.

For example, consent in the state of Florida expires after 18 months, making it so consumers have to opt-in again after that time to continue to receive messages. It is vital that organizations monitor consent expirations so that they can legally contact them again.

Regularly update consumer contact info

Periodically verify and update contact information to avoid contacting the wrong person. Consumers could change their phone number for any number of reasons. Since consent is tied to the person being called and not the actual phone number, it is important to ensure you are contacting the correct person you are intending to reach. To avoid violating compliance laws, make sure your consumer contact info is always up to date.

How you can prevent TCPA and DNC violations (continued)

Include clear opt-out information in all communications

Always include clear opt-out information in all communications and make the opt-out process simple and easily accessible. This way, your organization is complying with legal standards and respecting customer contact preferences.

Including clear opt-out information also enhances brand trust by giving individuals control over their communication preferences and builds a positive brand image.

Regularly train staff

Train employees regularly on TCPA compliance, including the latest regulations to avoid violating any laws.

It is especially important that customer-facing staff are aware of compliance protocols since they are the employees who will be talking to customers daily. With an educated staff, your organization is less likely to make compliance mistakes.

Conduct regular risk assessments

Periodically assess any potential risks related to TCPA compliance in your compliance strategy. Compliance rules and regulations are constantly changing, which means your strategy must be constantly updated as well.

Regularly assess your compliance strategy to address any identified risks to prevent issues.

Stay informed about industry changes and standards

It is important to stay informed about industry changes and standards when it comes to compliance, so your organization always remains aware of new regulations.

When new rules and regulations emerge, adjust your compliance strategy in a timely manner to ensure you remain compliant.

Is a compliance solution right for you?

To help protect your organization against the risks of violating TCPA and DNC regulations, consider implementing a compliance solution to eliminate risk across your entire organization.

Gryphon ONE is the only real-time, automated solution that mitigates risk of DNC and TCPA violations for all outbound communications. Gryphon AI's tier 1 carrier-grade network gets into the path of the call to block non-compliant interactions from any device, regardless of location, to safeguard your organization from making non-compliant calls.

Our solution leverages real-time updates and manages complex rules and regulations to ensure that you are always protected against federal, state, and local laws.

Are you ready to start your compliance journey? Contact us today at gryphon.ai/contact or call 617-279-2609.

About Gryphon AI

Gryphon AI is the gold standard for Intelligent Contact Compliance. We safeguard businesses from costly regulatory risks and unnecessary constraints on audience reach by delivering real-time insights and automated protection across every interaction.

Our platform offers real-time contact compliance insights before, during, and after every interaction to proactively identify vulnerabilities and opportunities. Because Gryphon ONE integrates seamlessly with your existing systems and solutions, you'll reduce complexity and ongoing costs while enhancing your compliance capabilities.

With two decades of experience serving highly regulated industries such as financial services, insurance, healthcare, and retail, we have maintained an impeccable record of $0 in fines while achieving a remarkable 97% customer satisfaction rate. Choose Gryphon AI and transform compliance from a fragmented challenge into a catalyst for growth.

Request a complimentary assessment today by visiting gryphon.ai/contact.

gryphon.ai