gryphon.ai

Ensure Compliance *Without Slowing Down* Outbound Calling

Do-Not-Call, TCPA, mobile, and more!

Ensure Compliance Without Slowing Down Outbound Calling

As the lines blur between personal and work phones with the growth of remote workforces, how can you ensure your sellers are in-compliance with Do-Not-Call (DNC) and Telephone Consumer Protection Act (TCPA) regulations without slowing down outbound calling?

Facing an unpredictable economy at the start of 2023, organizations prioritized positive customer experience to counter economic uncertainty. Now, top performing teams are continuing to prioritize brand reputation and risk mitigation while accelerating revenue growth. This means driving sales and churning out outbound calls; but **are your customer communications 100% compliant with DNC and TCPA compliance regulations?**

Without a compliance solution in place, your organization is at greater risk of costly penalties that you cannot afford to sacrifice in the current market. There have been increasing complaints of working professionals' personal cell phones being contacted, and you never know when a "professional plaintiff" – a consumer who will jump on the chance to sue – is lurking around the corner.

If you are taking on the risk of manually managing DNC and TCPA regulations in-house, it is vital to be aware of the myriad of evolving DNC and TCPA regulations at the state and federal levels – and that contacting consumers in violation of DNC or TCPA requirements can be detrimental to your brand.

gryphon.ai

To help safeguard your organization, this eBook explores:

1. **All sources of Do-Not-Call and TCPA risk for your organization, including contacting personal vs. work phone numbers, evolving state laws, and autodialers.**
2. **The benefits of investing in a compliance solution versus manual compliance management and data processing.**
3. **What type of solution is right for your organization, features to look for, and more!**

1. Understanding How Your Organization is at Risk

As business professionals are adopting hybrid routines or working fully remote, mobile phones have become a gray area in the marketplace.

While more employees are using their cell phones to conduct business while working from home, telemarketing to personal cell phones is occurring more often, stirring up uncertainty around DNC and TCPA guidelines.

Manual DNC Risk

If your organization is manually scrubbing lists and approving phone numbers for your sales team, you are at much greater risk of dialing a number on a Do-Not-Call list, whether it is accidental or due to a lack of full, in-depth compliance knowledge.

When your sales team prospects and contacts mobile phone numbers, there is no sign of differentiation between personal or business phone numbers on many of these lists. For B2B organizations, contacting a prospect's personal phone number while attempting to sell to their business makes your organization potentially liable for costly DNC violation penalties and consumer lawsuits.

If the individual is registered on the National Do Not Call Registry, your organization can be fined up to **$43,792 per illegal call.**

In addition to the National Do-Not-Call Registry, it is important to note that 12 states operate their own do-not-call lists: *Colorado, Florida, Indiana, Louisiana, Massachusetts, Mississippi, Missouri, Oklahoma, Pennsylvania, Tennessee, Texas, and Wyoming.*

Three states – *Colorado, Mississippi, and Pennsylvania* – allow organizations to enroll their business numbers on state DNC lists, meaning your organization can be fined for calling business numbers in certain jurisdictions.

Autodialer TCPA Risk

If your organization is making outbound calls using an automatic telephone dialing system (ATDS) or a system with the capacity to be an ATDS – even if you're not utilizing automated calling capabilities, without protections in place you are at high risk of violating TCPA guidelines by accidentally dialing a cell phone.

The TCPA requires that organizations using an ATDS or prerecorded messages when contacting consumer mobile numbers must obtain prior express written consent from consumers to legally contact them. Additionally, businesses must not use established business relationships (EBRs) to avoid getting consent from consumers.

This means that even if a wireless number is being used for business purposes, **you must obtain prior consent to contact the number if utilizing an ATDS**.

There is a common misconception that the TCPA doesn't cover B2B calls; while it seems like a gray area, B2B callers are not exempt from TCPA regulations. Violations of TCPA regulations result in penalties of $500 for each violation, and $1,500 for proven willful violations of the TCPA.

If that doesn't sound risky enough, a handful of states have enacted their own "mini TCPA" laws in recent years – including Florida, Washington, and Oklahoma – and it is anticipated that other states will continue to introduce their own state-level equivalents of the TCPA.

These rules add even higher levels of scrutiny and restrictions with reduced legal calling hours, clarification around what type of call constitutes a "telephone solicitation", and thresholds governing how many call attempts to an individual is allowed in a 24-hour period.

What does this mean for your organization? The TCPA does not preempt state laws, so it is imperative that businesses monitor both the TCPA as well as these recently enacted state calling laws and similar laws that are pending in state legislatures.

Avoid Cell Phone Lawsuits

As the lines blur between personal and business mobile phones with remote work, dual-use cell phones pose massive risk to organizations conducting outbound calling.

> In the case of **Chennette v. Porch.com Inc.**, plaintiffs Nathan Chennette and fifty other home improvement contractors argued that they have "residential [cell] phone numbers which [they] use in their home-based[ ] businesses," and that GoSmith Inc. (acquired by Porch.com, Inc. in 2017) sent 7,527 text messages to plaintiffs' cell phone numbers with an ATDS.
>
> In their business model, defendants GoSmith, Inc. and Porch.com, Inc., sell client leads to home improvement contractors. The lawsuit details that GoSmith Inc. sourced information from Yelp.com, YellowPages.com, and BBB.org, and sent automated text messages to the phone numbers of over ten million home improvement contractors – including contractors who had cell phone numbers listed for their businesses.
>
> All plaintiffs received more than one text message from GoSmith within a 12-month period without providing GoSmith their cell phone numbers or giving consent to receive text messages. Additionally, fifteen plaintiffs had numbers registered on the National Do-Not-Call Registry and received 2,754 text messages from GoSmith to their registered numbers.

It is vital to be aware that lead sourcing databases do not distinguish between personal and business mobile numbers. Further, while these databases identify if a phone number is on a DNC list, this won't necessarily prevent your salespeople from calling a registered number.

A sales operations admin must manually put these numbers into a Do-Not-Call bucket, but even this doesn't mean that your reps won't accidentally dial a number labeled DNC. While the information is there, it's up to each one of your salespeople if they use it or not. So why risk it?

Instead, with a compliance solution or failsafe process in place, your organization gains assurance that all calls violating DNC and TCPA requirements will be blocked.

Data Risk

With internal, wireless, state, and federal DNC lists, the reassigned number database, opt-outs, state holiday prohibitions, and state-of-emergency bans to keep up with, managing marketing compliance in-house is a large undertaking.

If that isn't enough, your organization cannot forget about client-specific business rules such as frequency of outreach, or more nuanced controls like determination of residency using zip code versus area code.

If your compliance process is not managed on a regular cadence, or in a centralized location, error in manual processing of these requirements or the time lapse between data change and data processing can result in costly penalties and brand damage.

For example, consider the complications associated with the Reassigned Numbers Database. Under the TCPA, consent applies to the consumer being called, not the phone number. This means that your organization will be held liable for contacting phone numbers for which they previously obtained consent to contact if the number has since been reassigned.

To avoid calling reassigned numbers, your organization must consistently scrub your contact databases to identify these numbers and avoid penalties.

If this sounds complicated to manage, it's because it is. Utilizing a compliance solution that can conduct a reassigned number scrub and identify these numbers is the only way to mitigate risk and avoid violations.

Instead of trying to navigate the myriad of constantly changing compliance regulations on your own, check out our **comprehensive marketing compliance checklist** to see all the ways your organization may be at risk of DNC and TCPA violations.

2. Investing in a Compliance Solution

Is your organization safe from costly fines and penalties that accompany all these compliance risks without a solution in place? Ensuring you have connectivity to a compliance platform across all internal and external calling platforms, whether using a dialer, phone systems, or cellular phones, can help mitigate risk for your organization. There are a variety of compliance solutions on the market that offer various degrees of protections, including:

- In-house systems
- List scrub services
- Automated, point-of-dial platforms

Regardless of device or access method used by your sales reps for outbound dials, a compliance solution will safeguard your team from DNC and TCPA violations. The right solution can help you:

- Prevent mistakes from inexperience or human error
- Minimize over-suppression of marketing contacts with custom controls tailored to your organization that improve your team's ability to sell
- Create full audit trails for peace of mind and ease of response

With a myriad of constantly changing state and federal DNC laws and TCPA regulations, **these are the top benefits that a compliance solution can provide for your organization:**

1. Automate DNC and TCPA compliance regulations to eliminate the risk of manual error.

A centralized, automated compliance solution can offer protection, safeguard consumer trust, and help increase revenue by eliminating over-suppression of valuable leads and outreach opportunities.

An automated solution gets in the path of every call your team makes to enable real-time, automated outbound call screening and blocking regardless of where calls are made or what type of device is used.

Every phone number is screened against TCPA, state, federal, company-specific business rules, and other Do-Not-Call lists so you don't have to devote valuable time and resources trying to keep up with the ever-changing compliance landscape.

An automated solution will ensure compliance with:

- FCC Telephone Consumer Protection Act
- FTC Telemarketing Sales Rule
- Federal Do-Not-Call lists
- State Do-Not-Call lists
- Ported Wireless and Wireless Number Blocks
- Internal Do-Not-Call lists
- Robocall and ATDS restrictions

If you only want to contact a consumer once a week, this type of solution will also automate that frequency, allowing your organization to devote fewer resources to preference management, eliminate human error, and allow your team to focus on generating revenue with peace-of-mind.

2. Centralize data management and auditing.

Who is managing federal, state, and internal Do-Not-Call lists, and state-by-state holidays, call curfew, and state-of-emergency restrictions for your organization? What processes do you have in place to ensure all outbound dialers, in-office and remote, adhere to your compliance process? And what audit processes do you have in place to demonstrate your compliance practices?

If you are internally managing list-scrubbing and outbound call data without a centralized management system in place, your business is at increased risk of manual error and costly DNC and TCPA violations.

You may even lack complete data reporting and a full, comprehensive audit trail for compliance – while years of calling information across your enterprise may be critical if ever faced with a consumer lawsuit.

If your organization makes outbound dials via cell phones, you will not have data to prove you tried to follow compliance restrictions if faced with a consumer lawsuit.

To play it safe, a compliance solution with centralized data management and integrated call capture provides key reporting and indisputable audit trails for complete peace-of-mind from costly violation penalties.

In the event of a lawsuit, a complete compliance solution will provide a record of all data, including when a transaction occurred, how the call was treated and why, and if that contact is on federal or state Do-Not-Call lists.

You can also access fully customizable reports for transparency into campaign, timeframe, sales rep, number of calls, talk time, average time/call, DNC blocks, DNC additions, and any configured result tags that your organization may need to evaluate.

3. Protect your company without prohibiting business from being conducted or slowing down revenue.

A top-tier compliance solution will offer personalization and customizable, business-specific controls to safeguard your organization while you increase revenue.

To prevent over-suppression of contacts, a compliance solution should be able to take advantage of legal exemptions and data hygiene opportunities under the law. This may include customizations for:

- Express or implied consent
- Established Business Relationships (EBRs)
- Removal of state and federal DNC list records that have changed ownership
- Expiration of opt-out records legally
- Consumer preference management and “opt-down” panels

Manually applying real-time timebound restrictions, such as call curfew blocks to certain contacts, and removing contacts that have opted to be put on a Do-Not-Call list – all within a legal timeframe – can be both risky and tedious.

Rather than risk human error or waste valuable resources manually honoring consumer protections, a compliance solution will simplify these processes.

Instead of worrying about compliance regulations and your brand reputation, leave it to the experts. A compliance provider will track the rules and update processes as needed, creating seamless integrations with disparate systems.

Investing in the right solution allows you to tailor compliance to your organization with custom controls to improve your team’s outreach abilities, and to create end-to-end efficiencies in your overall work- and call-flow process.

Rather than build out large IT technology and risk management teams to update and scale your systems to meet the ever-changing, hyper-regulated compliance landscape, a provider will do all that on your behalf and work to ensure your compliance program is as solid, scalable, and unintrusive as possible.

3. Features to Look for in a Compliance Solution

Whether you are considering an investment in a compliance solution to automate processes, centralize data management and auditing, or safeguard your brand reputation, there are a handful of factors to consider when choosing the right solution for your organization.

Consider the following: *What type of Integrations does this solution require to sync with your CRM and current tech stacks? Can this solution guarantee compliance for third parties making calls on behalf of your organization? Will this solution automate current in-house processes? Does this solution provide real-time call blocking for an extra layer of protection?*

To help determine what type of compliance solution is right for you, **here is a full list of features to consider:**

- Outbound call screening from any phone, used anywhere
- Call recording with transcription and redaction of sensitive information
- Timeliness and accuracy of data
- Source of the data
- Processes for protection from both federal and state law
- Frequency controls and other timebound restrictions
- Company-specific rules and requirements
- Data processing requirements
- Process for managing internal opt-outs
- Processes for managing EBRs/exemptions
- Pre-Call Whispers for legal disclosures required by law
- Audit reporting and reporting trails
- Redaction to ensure privacy

A top-tier solution will offer *Pre-Call Whispers*, voice prompts from the system, to inform agents of state-specific compliance disclosures required by law. This may entail "No Rebuttal" language allowed, "Permission to Continue" required, the called party "Must be 18," the caller must divulge that called party has right to "Opt-Out" from future calls, or the caller is calling an "All Party Consent" state.

gryphon.ai

Learn more

These days, it feels like you need a full-time legal team to keep up with the ever-changing compliance landscape. Is it allowed? Is it forbidden? Stop wasting time and money trying to figure it out on your own.

Gryphon.ai's real-time automated DNC and TCPA compliance platform delivers 100% warranted protection without over-suppressing legitimate contacts. The automated compliance platform checks every phone number at the point-of-dial against state, federal, and other Do-Not-Call registries, applies applicable exemptions, and blocks non-compliant calls automatically.

Contact (866) 665-2670 or sales@gryphon.ai to learn how Gryphon ONE can benefit your organization.