



HOW STRATEGIC
SILENCE WINS CASES

DEFENDING
DEPOSITIONS

STORYTELLING
WITHOUT WORDS

VOL. 52 NO. 2
WINTER 2026

Litigation

A PUBLICATION OF THE AMERICAN BAR ASSOCIATION
LITIGATION SECTION

Silence

TCPA Compliance, Litigation, and the Art of Saying (Almost) Nothing

BECKY ADAMS

The author is senior counsel at Gibson Dunn in Dallas. She previously served as chief legal officer at Quintessa Marketing.

The Telephone Consumer Protection Act (TCPA) is among the most potent sources of litigation risk in today's regulatory environment. The TCPA is a federal statute enacted in 1991 to restrict certain types of unsolicited communications, including autodialed calls, prerecorded voice messages, and marketing calls to numbers on the National Do Not Call Registry. The statute has two primary enforcement tracks: (1) restrictions on the use of regulated technology—such as automated telephone dialing systems or prerecorded voices—and (2) violations of Do Not Call list requirements. Each unlawful call, text, or voicemail can trigger statutory damages of \$500 per violation, with treble damages available for willful or knowing conduct. Moreover, most states now have their own “mini-TCPA” statutes that supplement the federal law, often with additional requirements, different definitions, and separate penalties. With a vibrant plaintiffs' bar eager to capitalize on technical noncompliance, companies large and small are frequently pulled into litigation over relatively minor communication missteps.

Yet, in this high-volume, high-liability landscape, the most effective defense is often not a dramatic courtroom strategy or an aggressive press release—it's restraint. Silence, when intentional and strategic, can be a powerful shield against TCPA liability. From quietly building airtight compliance programs to avoiding oversharing in pre-litigation negotiations, knowing what *not* to say, and when *not* to say it, can save companies millions.

This article explores how silence, applied wisely, can protect your company (for in-house lawyers) or your client (for outside

counsel) from becoming a target in TCPA litigation. It covers compliance design, negotiation posture, and litigation tactics that prioritize documentation over discussion, and discretion over demonstration. In the next installment, we'll examine the flip side: when it's time to make noise.

Consent Is Central

Silence begins with preparation, and in the TCPA context, preparation means building internal compliance systems that are both disciplined and defensible. At the foundation is consent—not just obtaining it but documenting it in a way that survives litigation. Whether the communication in question requires prior express consent or prior express written consent, companies must be able to show exactly how and when consent was obtained. That includes capturing the originating source, the precise language shown to the consumer, and a time-stamped record of the submission. It's not enough to rely on a general attestation that consent was secured. Courts expect specificity—and so do plaintiffs.

To meet this standard, many companies turn to third-party verification tools like Jornaya and ActiveProspect's TrustedForm. These platforms create independent session recordings or certificates that log the full HTML snapshot of the webpage or form where the consumer gave consent, along with key metadata such as internet address, user agent, and time stamp. These tools are especially valuable in high-volume lead generation environments, where manually re-creating each user's consent trail would be

impossible. But technology is only as good as the process that surrounds it. A company must ensure that consent records are centralized, accessible, and tied to the right consumer in a traceable way. When litigation strikes, silence is strongest when the documentation speaks for itself.

Equally important is the company's approach to opt-outs and suppression. The updated rules of the Federal Communications Commission (FCC) now require that companies honor all reasonable requests to stop communications, even if the consumer doesn't use "magic words" like "stop" or "unsubscribe." Any clear request to cease contact—whether via text, email, or even verbally—triggers an obligation to add that consumer to the appropriate do-not-contact list. These opt-out requests must be processed promptly and consistently, with suppression taking effect within 10 business days, as now required by FCC regulation. In practice, many companies now aim to update suppression systems within 24 hours to reduce risk and avoid accidental follow-ups.

Integration across communication channels is no longer just best practice—it's becoming a regulatory imperative. Currently, the FCC's updated rule allows companies to send a one-time confirmation text within five minutes of receiving a consumer's opt-out. This brief message can ask whether the consumer wishes to stop all communications or only a specific type, but it cannot be promotional in nature. However, if the consumer does not respond, the opt-out must be treated as global. And starting in April 2026, the FCC's "across-the-board" rule will codify this principle: Any opt-out request must be honored across all campaigns, subject areas, and communication types from that seller (subject, of course, to the one-time confirmation text). Companies will no longer be permitted to treat opt-outs as campaign-specific unless explicitly clarified by the consumer.

These developments require suppression systems that are not only fast but also comprehensive and centralized, ensuring that a single opt-out request silences all future telemarketing robocalls and robotexts—regardless of which department, product line, or third-party vendor initiated them. Forward-looking companies should begin preparing now by mapping data flows, tightening integration between platforms, and ensuring that internal "do not call" lists function as a unified control point for all outbound contact.

Record-keeping is the quiet backbone of TCPA defense. Companies should retain all consent and suppression records for a minimum of five years. Although the statute of limitations for private TCPA claims is generally four years under the federal catch-all rule, the Telemarketing Sales Rule enforced by the FTC imposes a five-year record retention requirement for certain telemarketing activities. Aligning retention policies with the longer of these two timelines not only ensures full regulatory compliance but also provides a buffer against litigation risk. Records should be preserved from the time of the last relevant activity—such as



the last call, opt-out request, or campaign use—and stored in a way that permits easy retrieval.

Compliance Requires Many Departments

TCPA compliance is not just a legal function; it must be operationalized. That means engaging information technology (IT), marketing, sales, and legal teams to ensure that data flows are mapped, that opt-out mechanisms are tested, and that consent capture isn't undermined by sloppy integrations or third-party gaps. The most prepared companies—those that build disciplined systems and operationalize compliance across functions—are the ones most likely to stay silent. And in TCPA litigation, silence is success.

This approach to internal compliance holds true regardless of industry. From business-to-consumer (B2C) marketing firms to health care systems, financial institutions, and even business-to-business (B2B) providers that mistakenly assume the TCPA doesn't apply, the need for quiet, verifiable systems is universal. Different sectors may face different regulatory overlays, but the core principles of TCPA risk management remain the same.

Regardless of industry, companies face real TCPA exposure—whether in B2C marketing, health care, financial services, or even B2B communications. While consumer-facing businesses are the most frequent targets of litigation, companies in sectors like health care, financial services, education, and even traditional B2B operations often overlook just how far the statute reaches. The danger lies in assuming that the nature of the message or the identity of the recipient exempts a communication from scrutiny. In reality, what matters most is the method of contact and the type of device involved.

A common pitfall arises in business-to-business contexts, where companies presume that professional outreach is categorically exempt from the TCPA. But in today's mobile-first world, that assumption is increasingly risky. Many professionals use their personal cell phones for work—either exclusively or as part of a bring-your-own-device environment. A marketing or informational call placed to what the sender believes is a

Illustration by Dave Klüg

“business number” may in fact reach a wireless device governed by the TCPA’s restrictions on autodialed and prerecorded communications. Given the blurred line between personal and professional use of mobile phones, businesses should proceed cautiously and avoid relying solely on assumptions about the nature of the number being dialed.

Highly regulated industries face additional complexity. Health care providers, for example, may be permitted under the Health Insurance Portability and Accountability Act (HIPAA) to contact patients for certain reasons—such as appointment or billing reminders—but that permission does not override the TCPA’s consent requirements. Courts have made clear that prerecorded or automated health care calls still require prior express consent, even if the message is HIPAA-compliant. The FCC has also reiterated that informational messages like prescription notifications fall under this standard, while any promotional content triggers the stricter rule requiring prior express written consent.

Avoiding liability starts with saying less, documenting more, and resisting the urge to explain.

Similarly, financial institutions must navigate overlapping duties under the TCPA, the Gramm-Leach-Bliley Act (GLBA), and the Fair Credit Reporting Act (FCRA). The GLBA requires institutions to deliver annual privacy notices and offer opt-out opportunities before sharing nonpublic personal information with non-affiliates, while the FCRA imposes notice requirements before using consumer credit data in certain contexts. These regulatory frameworks may operate in parallel, but they are not harmonized—and compliance with one does not ensure compliance with the others.

In this environment, cross-functional coordination is essential. Legal, compliance, marketing, and IT teams must align not just on the substance of what is sent but also on how, when, and to whom it is delivered. A failure to coordinate across these layers can lead to mixed compliance signals—and, ultimately, avoidable exposure.

Many Claims Should Be Resolved Early

Some TCPA claims are best resolved before they gain traction—especially when documentation is weak or further discovery may increase leverage for the plaintiff. When a company’s consent records are incomplete, outdated, or ambiguous, the risks of litigation often outweigh the benefits. Because consent is the cornerstone defense in TCPA litigation, the absence of solid documentation leaves a company exposed. Moreover, TCPA claims frequently pose class action risk. A single campaign-wide mistake can balloon into multimillion-dollar exposure if class certification is granted.

Claims originating from plaintiff-friendly jurisdictions further tilt the calculus toward early resolution. Certain courts have developed reputations for favoring broad interpretations of key TCPA terms and denying early motions to dismiss. If the facts involve a clear use of autodialers or prerecorded voice calls and if no viable motion to dismiss exists, silent settlement may be the most strategic move.

In addition, indemnity obligations must be considered. In some instances, the company named in a TCPA suit may not be the direct originator of the call or message but may have obtained leads or campaign support from third-party vendors. If those vendors provided contractual indemnification, settling early in some instances may allow for a smoother, lower-cost tender of defense or reimbursement claim without triggering protracted multiparty litigation. On the other hand, where indemnity provisions are weak or ambiguous, early settlement may help mitigate further exposure or cross-claims.

Companies with clean, verifiable consent records are often well positioned to mount a strong defense. Robust documentation can support early motions to dismiss or summary judgment, reducing exposure and litigation cost. But documentation alone isn’t the only factor that can tilt the scales in favor of litigation.

In many cases, the identity and behavior of the plaintiffs matter. Some plaintiffs—often referred to as “frequent flyers” or “serial plaintiffs”—have a history of manufacturing TCPA claims. These individuals may deliberately submit contact information across multiple lead forms or respond to ads with the intent of triggering a violation. The use of aliases or patterns of repeated filings suggests an intent to bait businesses into technical missteps. When the plaintiff is proceeding pro se, it’s particularly important to research the plaintiff’s litigation history. Adverse rulings in prior cases or a high volume of recent filings may provide valuable insight into the plaintiff’s strategy and tolerance for protracted litigation. Knowing your opponent can help tailor your defense and, in some cases, justify a more aggressive posture.

Another important consideration is the theory of liability. A claim for vicarious liability—where the company is accused of being responsible for a third party’s conduct—is often more

defensible than a direct liability claim. Plaintiffs asserting vicarious liability must prove an agency relationship, typically by establishing actual authority, apparent authority, or ratification. This higher burden provides defendants with several procedural and substantive avenues to challenge the claim. Courts may be more receptive to dismissing or narrowing the case early where the alleged third-party caller acted independently and without meaningful control by the defendant.

Favorable legal developments can also strengthen the case for defense. In *McLaughlin Chiropractic Associates, Inc. v. McKesson Corp.*, 145 S. Ct. 2006 (2025), the U.S. Supreme Court held that district courts are not bound by the FCC's interpretation of the TCPA; instead, they should apply ordinary principles of statutory interpretation, giving appropriate—but not controlling—weight to agency guidance. As a result, jurisdiction-specific precedent plays a growing role in litigation strategy. While evolving FCC guidance remains relevant, favorable case law within the applicable jurisdiction—or at least the circuit—often carries more weight in deciding whether to litigate or settle early. While these factors may favor a vigorous defense, they must still be weighed against broader strategic considerations. Even the strongest legal position can be undercut by steep litigation costs, unfavorable venue dynamics, or the potential for negative publicity. On the flip side, prevailing against a meritless claim—especially one brought by a frequent flyer or serial plaintiff—can reinforce the company's reputation and deter future lawsuits.

Offers made under Federal Rule of Civil Procedure 68, which shifts certain litigation costs if the plaintiff rejects a reasonable offer and fails to obtain a better outcome at trial, can be a useful tool to test a plaintiff's appetite for continued litigation. Ultimately, the decision to settle or fight should be grounded in evidence, economics, and strategy—not emotion. The best path forward is the one supported by documentation, diligence, and deliberate risk analysis.

TCPA plaintiffs often file vague or generic complaints that rely on boilerplate allegations—such as assertions that the call or text was made using an autodialer or without consent. Their goal is to survive early dismissal and move into discovery. Once the defendant starts sharing information about the defendant's systems or compliance protocols, plaintiffs adapt. They amend pleadings, shift factual narratives, and use disclosed data to reshape their legal theories, keeping defendants reactive and constrained.

Pre-Suit Talks

During early-stage negotiations, many defendants are tempted to share technical details or try to explain their compliance posture in hopes of avoiding a lawsuit. This approach often backfires. Providing consent documentation, disclosing how a number was obtained, or explaining lead generation pathways gives the

plaintiff a road map to reframe the case. Even sharing call volumes or dialer settings can lead to inflated allegations or creative pleading strategies.

The goal in pre-suit talks isn't to win the argument—it's to contain the cost. Instead of providing a road map to the plaintiff, focus negotiations on realistic valuation. What is the plaintiff plausibly entitled to under the TCPA's statutory damages scheme? What is the cost of ending the matter now versus proceeding through discovery?

Where appropriate, consider using narrow nondisclosure agreements to protect sensitive information exchanged during talks. And always assume that even protected settlement discussions may become discoverable. Although Federal Rule of Evidence 408 protects compromise offers from being introduced as evidence to prove liability, it does not shield underlying facts from discovery.

The most effective settlement posture is quiet strength. Don't overshare. Don't justify. Signal preparedness to litigate, but without advertising desperation to settle.

The value of a TCPA settlement goes beyond the dollar amount. A smart settlement agreement should include confidentiality provisions that cover not only the terms of the deal but its very existence. Plaintiffs should be barred from disclosing the agreement to third parties, including online forums, other litigants, or even attorneys, except as required by law.

Of course, enforcing confidentiality provisions presents practical challenges. A defendant may never know if the plaintiff quietly discloses settlement details to others unless the breach becomes public—such as a post in an online forum, disclosure during another lawsuit, or a tip from another litigant. But even limited enforcement potential can have value. Including a liquidated damages clause—paired with a clear definition of what constitutes a breach—can create a deterrent effect. Some companies also monitor known plaintiff-oriented online forums and legal communities to detect leaks. While it's difficult to police every communication, strong contractual language, paired with the possibility of financial consequences, may be the best bet to stop loose lips before they start.

Settlement Language

Every TCPA settlement should include language that closes the door on future litigation. Binding arbitration clauses can divert any subsequent disputes out of court and into a forum that favors confidentiality and efficiency. Just as critical, a well-drafted release should cover both known and unknown claims and be paired with a covenant not to sue. Unlike a release, which functions as a waiver of rights, a covenant not to sue creates an ongoing contractual obligation not to bring future lawsuits arising from the same underlying facts.

The scope of this covenant should be comprehensive. It should bar the plaintiff from asserting any claims—whether known or unknown, suspected or unsuspected—that arise out of or relate to the same events, communications, or transactions at issue in the settled case. It should also extend protection beyond the named defendant to include affiliates, agents, employees, customers, vendors, and other related entities that might otherwise be targeted in a follow-up suit. Courts generally enforce such covenants, particularly when they are supported by consideration and do not conflict with public policy. By combining a strong release with a clearly defined covenant not to sue, companies can better ensure that the settlement delivers lasting peace—not just a temporary pause.

Ultimately, the decision to settle or fight should be grounded in evidence, economics, and strategy—not emotion.

When dealing with serial TCPA plaintiffs, it's a good idea to include settlement terms that help prevent future claims. The agreement should require the plaintiff to disclose all phone numbers the plaintiff uses—whether residential, mobile, work-related, or otherwise—and impose a continuing obligation to notify the company of any newly acquired numbers. This allows the company to update its internal “do not call” list and reduce the risk of inadvertently contacting the plaintiff again.

The agreement should also include a notice-and-cure provision, requiring the plaintiff to give written notice of any alleged violation and provide a reasonable opportunity for the company to cure before initiating any further action. This clause can be styled either as a condition precedent to any future claim or as a waiver of the right to sue if the plaintiff fails to provide timely notice. In some cases, both mechanisms are used in tandem for added protection. Courts are generally willing to enforce these provisions if they are clear, reasonable in scope, and consistent with public policy.

Additional terms can further protect the company's reputation and litigation posture. Where enforceable, a non-disparagement clause may prohibit the plaintiff from making negative or harmful public statements about the company or its affiliates. A noncooperation clause may restrict the plaintiff from voluntarily assisting

other attorneys, plaintiffs, or regulators in pursuing similar TCPA claims. This doesn't preclude compliance with lawful subpoenas, but it does limit the plaintiff's ability to serve as a springboard for coordinated litigation. These clauses must be drafted with care to avoid overbreadth or constitutional concerns, but when properly tailored, they can provide valuable insulation against repeat targeting.

Courts generally respect clearly drafted settlement terms, especially when negotiated between represented parties. But even when a plaintiff is pro se, that doesn't necessarily indicate inexperience or a lack of sophistication. To the contrary, many serial TCPA plaintiffs are extremely legally sophisticated, having filed dozens of lawsuits and developed a strong familiarity with the statute and litigation process. Courts increasingly recognize this distinction, making it more likely they will enforce settlement provisions when the terms are clear, reasonable, and mutually agreed upon.

Plaintiffs and their counsel often expect minimal run-of-the-mill agreements; detailed settlements can catch them off guard and reduce their willingness to repeat the cycle. Ultimately, the goal is not just to resolve a single case but to prevent a cycle of opportunistic litigation. Well-crafted settlements can turn one-time costs into lasting safeguards.

Silence in litigation doesn't mean weakness—it means precision. Plaintiffs bear the burden of pleading and proving key elements, such as lack of consent, use of an automated telephone dialing system, or receipt of a prerecorded message. In some cases, it may be unwise to affirmatively present your consent evidence early in the case. Let the plaintiff commit to a narrative, and then use motions to dismiss, jurisdictional challenges, or discovery to test the plaintiff's claims before you reveal your strongest cards.

Discovery should be approached carefully. Rather than volunteering information that could educate or embolden your opponent, use the process to identify inconsistencies, overreach, or a lack of factual support. In many instances, keeping your defenses close can maximize leverage—especially when plaintiffs are overplaying a weak hand.

That said, not every case calls for silence. There are moments when making noise is the best strategic option—whether through a Rule 11 motion, a counterclaim, or public-facing litigation tactics. Next issue, the second article in this series will explore those scenarios and how to turn the tables on serial litigants through strategic disruption.

In the world of TCPA compliance and litigation, silence isn't a sign of passivity—it's a disciplined strategy. The most successful companies are those that prepare quietly, negotiate discreetly, and litigate with surgical precision. Through robust documentation, restrained disclosures, and thoughtful settlement structures, they avoid becoming targets or—worse—examples. ■

Becky Adams can be reached at badams@gibsondunn.com.