TCPA Compliance 101: Managing the Surge in TCPA Filings

Queenie
Puja J. Amin

TCPA AND MINI-TCPAS ARE A MASSIVE COMPLIANCE & BRAND RISK

TCPA may be the single greatest legal risk your institution faces

- Many times, institutional knowledge is not what you'd expect
- Lots of diffuse stakeholders, systems and data, evolving case law & regulatory guidance, make the job of identifying risk challenging
- Taking a holistic view of operations and setting policies and procedures is a must
- Risk goes **beyond** litigation — your BRAND is at issue anytime you face a "Robocall" lawsuit
- To build and maintain a reputable brand and maintain customer satisfaction, you must give your customers the respect they deserve

Contact Us Now

HOW TO IDENTIFY TCPA RISK – THINGS TO THINK ABOUT

- You need to have a sense of **ABSOLUTELY EVERY FORM OF CONSUMER OUTREACH.** Blind spots are **death.**
- **What states are you operating in?**
- What business functions reach out to customers?
  - For what purpose?
  - Using what channels?
  - Using what systems?
  - What business stakeholders own these operations?
  - Who is able to make changes—deploy new campaigns or outbound strategies?
- Make sure someone in legal or compliance OR your outside counsel is consulted before any marketing campaigns are changed

UNDERSTANDING CALLING SYSTEMS AND DATA

- Technology can be scary for most lawyers but assuring TCPA compliance requires in house compliance professionals (and outside counsel) to be FEARLESS in gaining knowledge of platforms and data systems
- For each outreach method your enterprise engages in, legal needs to know:
- What platforms are being used for what outreach efforts and under what circumstances?
- What systems of record are being used to pull data from? Using what criteria? (And who sets those criteria?)
- What systems store dispositions and transactional dialer logs after calls are made?
- What data sets exist around consent, wrong numbers, revocation?
- How is the internal DNC list being maintained for marketing purposes?
- Call recordings?
- Legal/compliance should set intelligent standards regarding document retention—don’t just hold data for no reason.

ATDS CASES ARE STILL LURKING IN 2025:

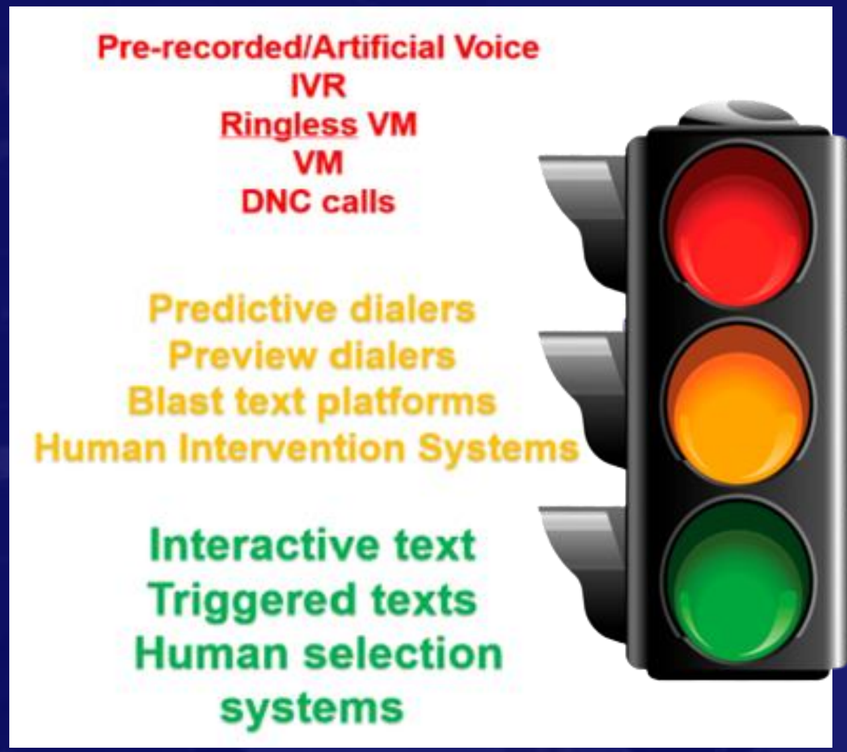
UNDERSTANDING CALLING SYSTEMS AND DATA

- Most courts interpret the phrase “equipment which has the capacity” to mean that if a system is capable of functioning as an ATDS, all calls—manual or not—may be treated as ATDS calls, regardless of how the call was actually made
- Jurisdictional differences in defining “capacity” create further compliance risk.
- Recent cases (*Frato, Ioszpe, Taylor*) show that allegations of “click and pause,” number rotation + SMS unsubscribe features can survive early dismissal—making it critical to understand your calling systems
- Key Indicators of an ATDS include:

  1) Using a random or sequential number generator **to generate** telephone numbers that are actually called as part of a campaign.

  2) Using a random or sequential number generator **to select** phone numbers to be part of a dialer file from a larger list of numbers.

  3) Using a random or sequential number generator **to determine the order** in which stored telephone numbers will be dialed.



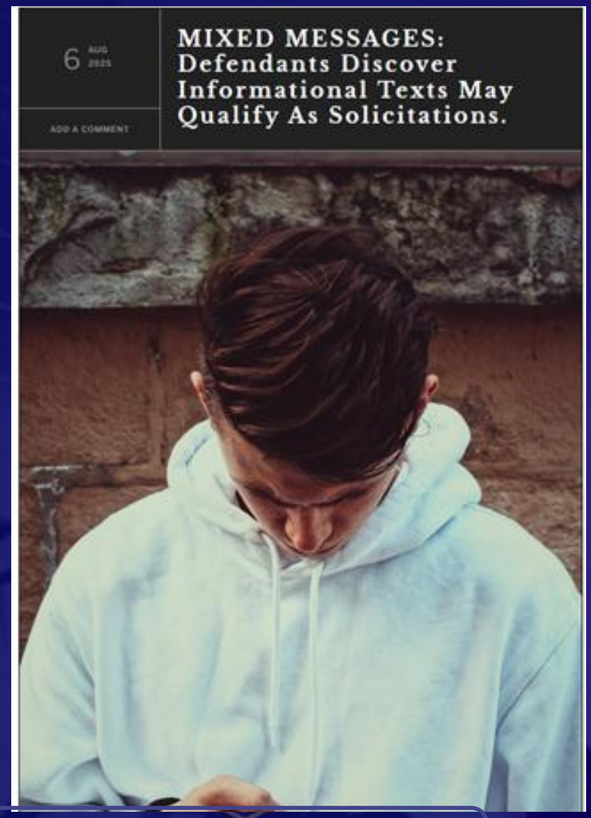
INFORMATIONAL V. MARKETING: 2025 CASE TRENDS

MIXED MESSAGES: "INFORMATIONAL" TEXTS MAY STILL COUNT AS SOLICITATIONS

- Courts continue to scrutinize message content closely to determine whether a communication is “marketing” under the TCPA
- In ***GERMAIN v. MARIO'S AIR CONDITIONING & HEATING,*** the court held that even a **HURRICANE SAFETY REMINDER** text could qualify as a **TELEPHONE SOLICITATION.**
- The message — "We are here for you" plus a **PHONE NUMBER** — was enough to **ENCOURAGE COMMERCIAL ACTIVITY**
- The court ruled that **INFORMATIONAL AND PROMOTIONAL MESSAGES ARE NOT MUTUALLY EXCLUSIVE**
- **In *Abboud v. Circle K,* a double opt-in message inviting users to receive “special offers” was deemed potentially marketing**
- **In *Germain*, even a storm safety reminder was treated as marketing due to its business tie-in**
- **In contrast, *Rockwell* held recruitment calls are not solicitations, and *Zipongo* found that third-party funded service notifications are informational, not marketing.**
- Review all "informational" texts for **IMPLIED SALES LANGUAGE** before sending – AVOID dual purpose messages without proper level of consent
- Even messages with helpful or neutral content can be considered marketing if they have a commercial purpose or promotional language

Informational VS. Telemarketing

- Dual purpose calls are
- BUT informing a customer of a service they've already purchased is not telemarketing
- Responding to a consumer's specific request for information is not telemarketing; but response cannot exceed scope of original request.
- Calls or texts to complete a "transaction" that has begun online—such as reminders to complete a webform— are not telemarketing.
- Informational: Just needs to be provided by the consumer to the caller for a purpose "closely related" to the purpose of the call.
- Immediate responses to consumer-initiated requests for information are not marketing.



If your text CREATES A COMMERCIAL PURPOSE or PROMOTES YOUR BUSINESS, it can be treated as MARKETING UNDER THE TCPA.

CONSENT CHEAT SHEET

	LANDLINE		CELLPHONE	
	Marketing	**Non-Marketing (Informational)**	**Marketing**	**Non-Marketing (Informational)**
Autodialed Calls/ Texts	If no prior express written consent, must scrub against National Do Not Call List	No restriction	Prior express written consent with opt out and conspicuous disclosure	Prior express consent
Artificial/Prerecorded Voice/ Use of Artificial Intelligence	Prior express written consent with opt out and conspicuous disclosure	Depends on content – call restrictions apply	Prior express written consent with opt out and conspicuous disclosure	Prior express consent
Manually Dialed	If no prior express written consent, must scrub against National Do Not Call List (or have an EBR/inquiry)	No restriction	If no prior signed express written consent, must scrub against national Do Not Call List (or have an EBR/inquiry)	No restriction

CALLER ID REQUIREMENTS – PRIVATE RIGHT OF ACTION!

Failure to properly transmit Caller ID can now trigger lawsuits and $500 statutory damages per call or text.

- Any person or entity engaging in telemarketing must transmit Caller ID information, including: the Calling Party Number (CPN) or Automatic Numbering Information (ANI)
- If your telecom carrier allows it, always display your entity's name in Caller ID
- You may transmit the name of the seller you're calling on behalf of, ***if:*** the number shown allows recipients to call/text back during business hours & the number supports DNCs
- According to recent case law, must transmit caller ID information with your text messages as well.
- It is unclear what this means – one read is that you have to supply your name in the content of the text message. However that is not necessarily what the regulation states – the law itself is vague.
- It simply says any telemarketing call must include the caller ID information *if* the carrier makes it available.
- Where branding services require a per-call fee, it is currently an open legal question whether not using such services violates the law and not using the paid service may still cause TCPA risk

TROUTMAN AMIN, LLP

NEW LITIGATION RISK: Liability from Non-Compliance with the TCPA's Caller ID Requirements

In the first ruling of its kind, a federal court in Michigan held that 47 C.F.R. § 64.1601(e), regarding Caller ID Requirements, confers a private right of action under the TCPA, meaning **penalties of $500 per non-compliant call or text, or up to $1,500 per knowing or willful violation.**

The Rule: Caller ID Requirements

Two requirements, under § 64.1601(e), for all telemarketing **calls and/or text messages**:

1. **PHONE NUMBER DISPLAY REQUIREMENT**: Transmit outbound **telephone number**
   - The phone number may be substituted for the telemarketer's customer service phone number
   - Blocking or hiding the outbound phone number is not permitted
2. **NAME DISPLAY REQUIREMENT**: Display the **name of the telemarketer** by displaying either:
   - The name of the telemarketer on the recipient's Caller ID OR
   - The name of the seller on behalf of which the telemarketing call is placed on the recipient's Caller ID

A Requirement for a Branded Caller ID Solution?

- § 64.1601(e) requires displaying the name of the telemarketer "when available by the telemarketer's carrier"
- This regulation was drafted in 2003—now, in 2025, there is little doubt about the availability of Caller ID
- Whether through a carrier or a branded Caller ID solution, the regulation requires a name to be displayed

The above requirements are for **all telemarketing**, regardless of whether there is any type of consent and regardless of even an established business relationship.

The Risk: MASSIVE LIABILITY

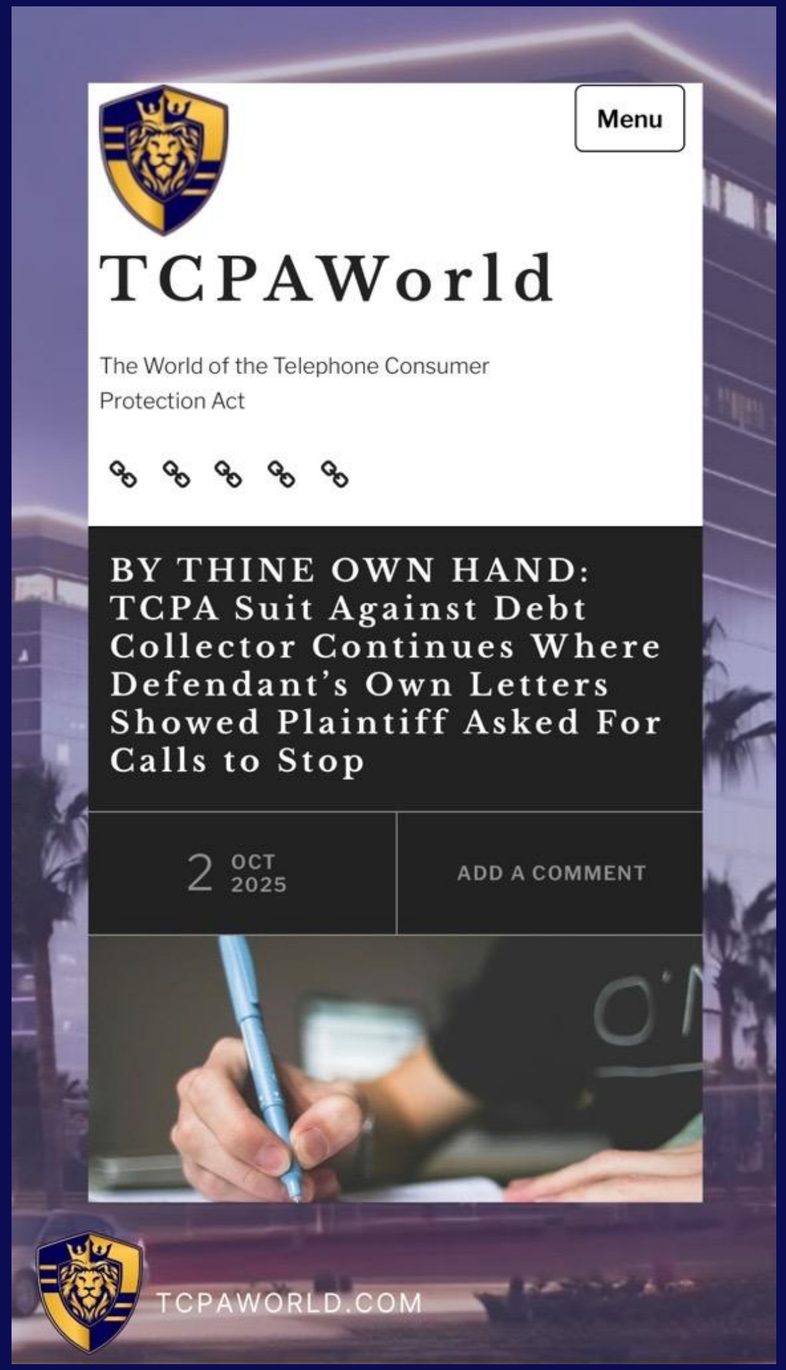
- With a private right of action, plaintiffs may bring **class action** claims with **each call/text** creating liability of:
  - $500 per violation (meaning **every** call or text that does not comply with the above requirements)
  - $1,500 per knowing or willful violation
- If you are not showing Caller ID, a class could include **all of your telemarketing call and text recipients**

The Origin: a Ruling in Michigan

- It was the first ruling of its kind, as a federal court in Michigan held that the Caller ID Requirements confer a private right of action under the TCPA, thereby allowing a plaintiff to sue for past Caller ID violations
- The Michigan ruling is the minority view, as every previous ruling has gone the other way, but it shows that you can be held liable for violating the Caller ID Requirements—and other courts may follow suit

Next Steps: Review Your Calling Practices

1. Are you **showing your business name** for all calls and text messages?
   - If you, **are not**, you may be **violating** the Caller ID Requirements
     - Check to see if your carrier or dialing system supports showing your name on the outbound Caller ID
       - If not, you may need to look into a branded Caller ID solution to comply with the requirements



HUGE WAVE OF 2025 REVOCATION CASES

"DO NOT SEND ME ANYMORE MESSAGES!!!!" — THE NEW FRONTIER OF TCPA LITIGATION

- A surge of **TCPA CLASS ACTIONS** is targeting major brands over **NON-KEYWORD SMS OPT-OUTS** — phrases like "Do not send me anymore messages" or "I do not wish to be contacted."
- FCC determined using the words "stop," "quit," "end," "revoke," "opt out," "cancel," or "unsubscribe" ok–BUT "does not preclude, use of other words and phrases to revoke consent." FCC will look at "totality of the facts and circumstances surrounding the specific situation…"
- FCC confirmed that consumers may revoke consent in any reasonable manner that "clearly expresses" a desire not to receive further calls or text messages—caller CANNOT dictate exclusive means to revoke consent that precludes the use of any other reasonable method

Contact Us Now

IMPLEMENTING POLICIES, PROCEDURES AND TRAINING:

- Proper DNC procedures help avoid violations, reduce litigation exposure, and demonstrate regulatory good faith.
- While phrases such as “not interested” do not qualify as a DNC request, a consumer is not required to formally request their number be added to a DNC list to trigger a DNC. Any request that “calls stop” or the like should be dispositioned as a DNC and policies should reflect the same
- Develop a training program covering: how to correctly log DNC requests; difference between “Not Interested” vs. “Do Not Call”; Handling verbal **and written** DNC requests from all channels of communication
- Bad/incomplete policies (or no policies) create gaps that can lead to certification in a class action and massive damages
- This is how you defeat certification. Policies are your sword and your shield in litigation.
- Plus, failure to maintain Internal DNC policies enables direct private right of action and possible damages
- **REMEMBER TO SET PROCEDURES AROUND STATE LAWS AS WELL**—time restrictions, state DNC lists; oral disclosures etc.

LEAD SELLERS WON'T SAVE YOU

- So often your best compliance efforts stop at the door. As soon as you turn to vendors you take on risk.
- **Lead vendors love to promise "TCPA compliant leads"... until there's a LAWSUIT**
- **KNOW YOUR VENDORS**: Relationships matter. Get to know people face to face. And get intel from people you trust.
- **DO NOT JUST RELY ON BUSINESS RELATIONSHIPS IN VETTING VENDORS.**
- Organizations like R.E.A.C.H. can help you identify solid lead vendors
- Remember, lead fraud and improper consents are the biggest risks facing many institutions
- Absolutely essential to have vendor intake controls residing with legal/compliance
- In one case, **Liberty Mutual** spent **over $1.3 MILLION** defending TCPA class actions after **All Web Leads** allegedly **refused to indemnify or defend.**
- Absolutely essential to have vendor intake controls residing with legal/compliance
- Regular vendor intake process is not going to be robust enough to spot all the critical TCPA ISSUES
- Use EXTENSIVE questionnaires before onboarding a vendor and do due diligence
- Remember lead fraud and improper consents are the biggest risks facing many institutions

If your compliance plan is "THE LEAD VENDOR SAID IT WAS FINE," you DON'T HAVE a compliance plan.

REDUCING TCPA RISK WITH ENFORCEABLE ARBITRATION TERMS

- Arbitration clauses and class action waivers provide a more efficient, confidential, and cost-effective way to resolve disputes, and may be particularly helpful in reducing exposure arising from TCPA claims.
- Courts increasingly enforce arbitration agreements, especially when properly disclosed and accepted.
- Use clear & conspicuous language in agreements & disclosures
- Class Action Waiver: explicitly bar class actions (user must be clearly informed)
- Delegation of Covered Parties: define parties broadly to include affiliates, marketing partners and agents.
- Obtain affirmative assent (checkbox + hyperlink terms).
- Terms of use hyperlink is in a distinctive color (preferably blue) and underlined.
- Maintain records of user acceptance (but be careful with CIPA risk).
- Review terms for state law enforceability (e.g., unconscionability standards may require an opt out mechanism).
- Regularly update terms to reflect evolving TCPA and arbitration law