

TCPA Claims: FCC Guidance on Key Provisions Remains Elusive

By Matthew J. Tharney, Natalie S. Watson and Elizabeth Monahan

Enacted to prevent costly calls to cell phones at a time when most Americans did not own them, the Telephone Consumer Protection Act of 1991 (TCPA), 47 U.S.C. §227, prohibits the use of automatic telephone dialing systems (ATDS) to call or send text messages to a called party without the “prior express written consent” of that called party. 47 U.S.C. §227 (b)(1) (iii). In its Sept. 15 written comments to the U.S. House of Representatives, Committee on Energy and Commerce, the U.S. Chamber’s Institute for Legal Reform (ILR) reported a 940 percent increase in TCPA class action claims filed between 2010 and 2014. ILR also noted that 3,710 TCPA class action claims had been filed in federal court in 2015 alone.

The Federal Communications Commission’s (FCC) July 10, 2015, Omnibus Order was meant to expand safe harbor provisions and allow industry to better understand compliance obligations. Instead, since the Order was issued, there have been more questions than answers for companies using telemarketing calls. This article provides an overview of key legal issues and current trends in TCPA litigation for companies who direct their marketing efforts to cell phones using ATDS technology.

The TCPA Generally: Automatic Penalties Regardless of Intent

TCPA prohibits telemarketers from using ATDS-functional equipment to place a marketing call to a cell phone without the prior written consent of the called party. The TCPA provides in pertinent part:

It shall be unlawful for any person ... to make any call (other than a call made for emergency purposes or made with the prior express consent of the called party) using any automatic telephone dialing system or an artificial or prerecord-

ed voice ... to any telephone number assigned to a paging service, cellular telephone service, specialized mobile radio service, or other radio common carrier service, or any service for which the called party is charged for the call.

47 U.S.C. §227(b).

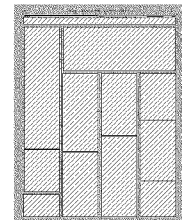
The TCPA defines an ATDS as “equipment which has the capacity (A) to store or produce telephone numbers to be called, using a random or sequential number generator; and (B) to dial such numbers.” 47 U.S.C. 227(a)(1). FCC clarified that dialing equipment that has the *capacity* to store, produce and dial numbers at random or sequentially, even if not presently used for that purpose, qualifies as an auto-dialer. *See* FCC Omnibus Order, at ¶111.

Under the plain wording of the statute, a misdialed number is sufficient to trigger a violation. The TCPA is a strict liability statute that awards \$500 per violation, and up to \$1,500 per willful violation, per call. Given those automatic penalties, violations under the TCPA can lead to significant potential exposure.

The Real Defense Is a Good Offense: Confirming “Prior Express Consent”

Documenting “prior express consent” is the key statutorily recognized defense to a claim under the TCPA. The FCC has defined “prior express written consent” to mean “an agreement, in writing, bearing the signature of the person called that clearly authorizes the seller to deliver or cause to be delivered” the ATDS call or text to the called party’s cell phone. 47 C.F.R. §64.1200(f) (8)(i). The “written agreement” must include a “clear and conspicuous” disclosure authorizing the ATDS call while also advising that the called party is *not* required to sign the agreement, directly or indirectly, or to agree to enter into the agreement as a condition of purchasing any property, goods, or services. *Id.* at 64.1200(f)(8)(ii).

• *Practice Tip:* We recommend that



companies retain proof of each called party's signed consent to receive ATDS calls. Such documentation should be maintained for the four-year statute of limitations that applies to the TCPA. Upon learning of a TCPA claim, the company should conduct due diligence immediately regarding the named plaintiff and calls made by the company during the time period alleged in the claim, to allow the company to demonstrate compliance and evaluate potential exposure.

Written Consent Via Electronic Signature

The term "signature" is defined to include "an electronic or digital form of signature, to the extent that such form of signature is recognized as a valid signature under applicable federal or state contract law." *Id.* Thus, the validity of the called party's electronic signature will vary state to state.

Moreover, FCC's Order suggests that consent to a website's terms of use may be insufficient to establish prior written consent under the TCPA. *See generally id.*, at ¶52.

- *Practice Tip:* We recommend that companies design their websites so that a toggle box or similar interface is included through which the prospective client can confirm consent with a check or through other written submission.

The Danger of Dialing a Wrong Number

FCC requires that the calling party obtain consent from the cell phone's "current subscriber" or "the non-subscriber customary user of the phone." *Id.* Cell phone numbers for many "pay as you go" devices, however, regularly are recycled to other customers.

Many petitioned FCC to carve out a safe harbor exception for inadvertent or other wrong numbers. FCC rejected those efforts, offering a much more limited safe harbor. *Id.* at ¶¶73-75. FCC will not impose the automatic statutory penalty for a single call if the calling party can show that the number was reassigned from a prior user who provided express written consent. The calling party has only one call or text to learn of the reassignment. If there is no response from the called party and that

party is called again, that second call to the reassigned number will trigger the penalty.

- *Practice Tip:* To guard against exposure posed by inadvertent calls to reassigned numbers, FCC suggests that an interactive opt-out mechanism be included in all artificial voice calls for reporting a reassigned number, along with establishment of policies and procedures to deal with reassignment of phone numbers. *Id.*, at ¶86. Documentation of those policies should be maintained to demonstrate the attempt to comply and to better defend against claims of willful violation of the statute.

Revocations and Opt-Outs

In its Order, FCC reiterated that consumers have the right to "opt-out" or revoke their earlier consent through any "reasonable method." *Id.* at ¶64. FCC failed to provide any bright-line rule to determine reasonableness. Instead, FCC advised that no "undue burdens" should be placed on the called party in revoking prior consent. "Reasonableness" will be decided on a case-by-case basis, based upon the "totality of the circumstances." *Id.* at ¶64, n. 223. Examples of "reasonable methods" include revocation by a called party "by way of a consumer-initiated call, directly in response to a call initiated or made by a caller, or at an in-store bill payment location, among other possibilities." *Id.* at ¶64. Thus, arguably, any customer walking into one location of a national department store chain can revoke consent while paying their credit card bill with the cashier.

- *Practice Tip:* We recommend that companies document revocation and opt-out policies and provide notice of those policies to their employees.

The Unclear Status of "App Developers"

Through its Order, FCC purported to offer a safe harbor exception for certain "App Developers" whose technology is used to make calls. *Id.* at ¶28. FCC's language, however, makes it difficult to determine prospectively whether the safe harbor will apply. FCC offers only a general, "totality of the circumstances" exception to the automatic penalty provisions. The test under the regulations requires analyzing the total-

ity of facts and circumstances, including an evaluation of who took the physical steps of placing the call and whether anyone else could be considered to have initiated the call. Liability will attach if the technology at issue “willfully enables fraudulent spoofing of telephone numbers or assists telemarketers in blocking Caller ID, by offering either functionality to clients” or “offers a calling platform service for the use of others has knowingly allowed its client(s) to use that platform for unlawful purposes.” *Id.* at ¶108.

• **Practice Tip:** Protection under the safe harbor provided to “App Developers” remains unclear. Developers should conduct a detailed review of the application’s terms of use and any operative contractual provisions with users to ensure compliance with FCC’s regulations to the greatest extent possible, given the ambiguities inherent in the regulations.

Conclusion

In sum, a year after FCC’s Order,

companies engaged in telemarketing are no closer to receiving critical guidance from FCC. Indeed, FCC’s Order currently is being challenged in the Second and Ninth Circuits. See *ACA International et al., v. FCC*, No. 15-1211 (D.C. Cir. 2016); *King v. Time Warner Cable*, No. 15-2474 (2d Cir. 2016); *Sterling v. Mercantile Adjustment Bureau*, No. 14-1247 (2d Cir. 2016); *Marks v. Crunch San Diego*, No. 14-56834 (9th Cir. 2016). Until further guidance is provided, companies must be ever-vigilant in documenting compliance with FCC’s implementing regulations. ■

Tharney is a partner at McCarter English and a Certified Civil Trial Attorney with a diverse complex civil litigation practice, including the defense of class actions. Watson is a partner at the firm, defending pharmaceutical corporations, manufacturers and health-care facilities in regulatory and compliance challenges. Monahan is an associate at the firm.



PHOTO BY ANDREW HARNIK