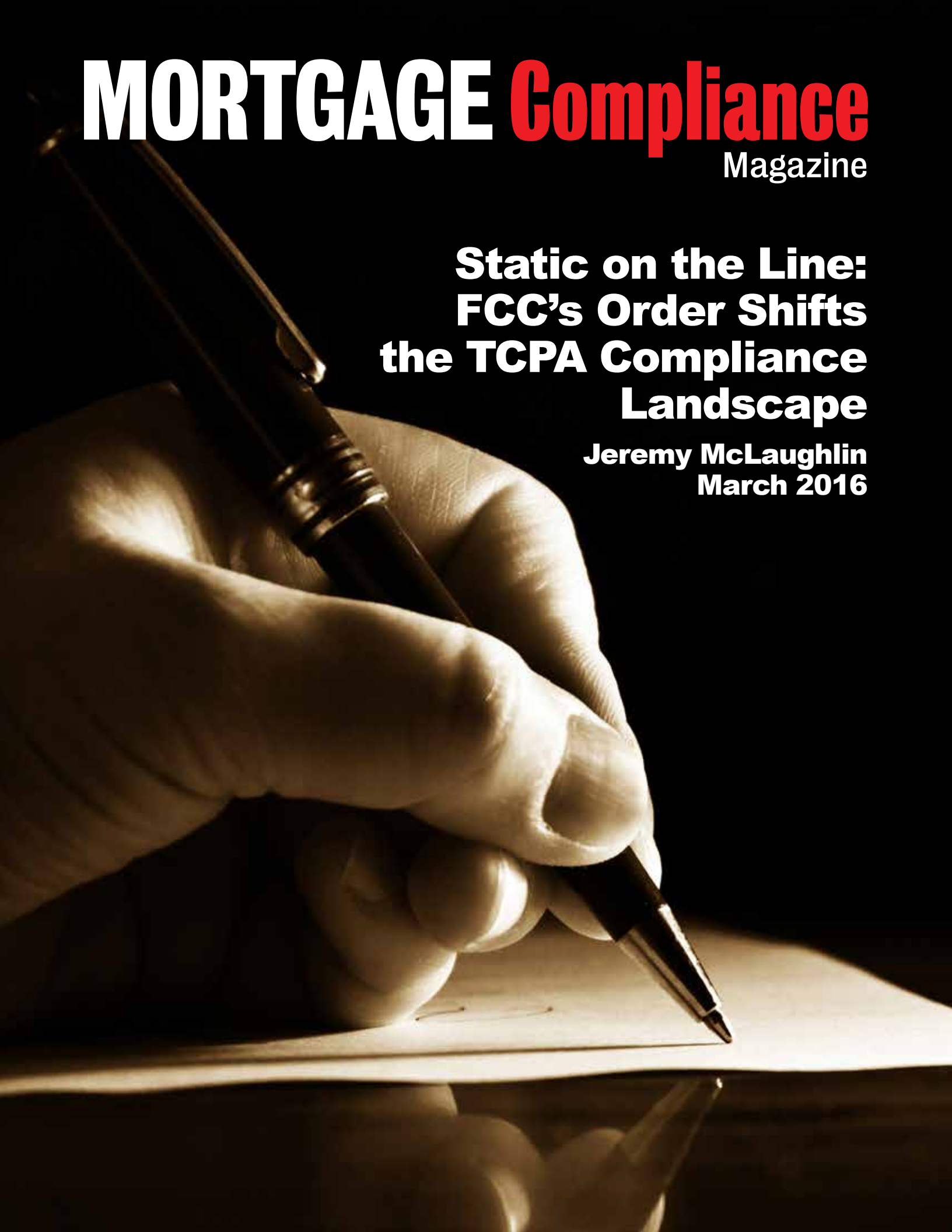
MORTGAGE Compliance
Magazine



# Static on the Line: FCC's Order Shifts the TCPA Compliance Landscape

Jeremy McLaughlin
March 2016

# *Static on the Line:* FCC's Order Shifts the TCPA Compliance Landscape

BY JEREMY MCLAUGHLIN

Jeremy McLaughlin

**Over the past 25 years and especially in the past decade, the TCPA has become a particular focus of plaintiffs' attorneys. That trend shows no signs of abating.**

Congress enacted the Telephone Consumer Protection Act (TCPA) in 1991 to address perceived problems created by unsolicited telemarketing calls and faxes. Over the past 25 years and especially in the past decade, the law has become a particular focus of plaintiffs' attorneys. The number of TCPA lawsuits filed in 2009 was well below 500, whereas there were almost 2,500 filed in 2014 alone. That trend shows no signs of abating. What's more, these cases are nothing to sneer at. A plaintiff may recover up to $500 per TCPA violation, which may be tripled if the violation is willful or knowing. Because many TCPA actions are filed as putative class actions, those numbers can add up quickly. Recent TCPA cases have settled for as much as $75 million.

So, what does all this mean for mortgage companies? Compliance is essential—and not just surface level compliance. Recent regulatory action and case law makes clear that regulators and courts will focus on macro level compliance with issues such as consent and revocation. This is particularly important for mortgage companies making promotional or servicing related calls.

The focus of this article is to provide compliance professionals with an introduction to some key TCPA compliance considerations. The TCPA imposes numerous requirements and governs a variety of technologies for communicating with consumers in a variety of contexts. For example, the TCPA is the genesis of the federal "Do Not Call" list and related requirements. In order to provide specific, macro-level compliance information, however, this article will focus only on some of the key issues raised by a recent Federal Communication Commission (FCC) rulemaking. As a result, this article will not address all the TCPA's requirements and should not be relied on for a comprehensive compliance program.

## FCC 2015 ORDER

On July 10, 2015, the FCC issued a much-anticipated Declaratory Ruling and Order (the Order) in which it "clarified" numerous aspects of the TCPA. The Order was effective immediately. Despite its purported purpose of clarifying TCPA requirements, the Order imposed additional requirements on businesses in a variety of circumstances. This article will focus on the following compliance issues: (1) what is an "automatic telephone dialing system" (ATDS); (2) who must give consent; (3) who can revoke it; and (4) financial institution exceptions. Some other topics addressed in the Order include who is the maker of a call, Internet-to-text messages, and call blocking technology.

## WHAT IS AN ATDS?

Among other things, the TCPA makes it unlawful for any person to make a call using an ATDS to any telephone number assigned to a cellular telephone unless that person has the prior express consent of the called party. It is crucial, therefore, to determine whether a company's technology qualifies as an ATDS.

The statute defines an ATDS as "equipment which has the capacity to store or produce telephone numbers to be called, using a random or sequential number generator; and to dial such numbers." Previously, the FCC opined that dialing equipment with the capacity to predictively select and dial telephone numbers that are stored in a database is an ATDS and so is a "predictive dialer" to the extent it has the capacity to dial numbers randomly or sequentially. The Order suggests, however, that these (and other) technologies qualify as an ATDS simply by having the capacity to store or produce and dial random or sequential numbers, even if the technology is not currently used for that purpose. Technology is not excluded from the definition of ATDS simply because it lacks the "present ability" to dial randomly or sequentially; it is not the current configuration of the technology that matters, but rather its "potential functionalities." So, for example, even if equipment requires a software update in order to dial random or sequentially, it could qualify as an ATDS if it has the potential to be modified so as to function as a random or sequential number generator and to dial those numbers.

Although the Order significantly broadens what may qualify as an ATDS, the FCC noted that there are some limits. The ability to dial numbers without human intervention, the Order explained, is the hallmark of an ATDS. But how the human intervention element applies "is specific to each individual piece of equipment" and, therefore, how that element weighs in the ATDS determination is a case-by-case review. The Order attempted to set an "outer limit" on what qualifies as an ATDS by stating that not "every piece of malleable and modifiable dialing equipment that conceivably could be considered to have some capacity, however small, to store and dial telephone numbers" qualifies as an ATDS; "otherwise, a handset with the mere addition of a speed dial button" would qualify.

Companies need to closely examine their technologies to determine whether they qualify as an ATDS. Some courts have already faced such questions in light of the Order, and the results have been mixed.

## WHO MUST GIVE CONSENT?

Consent, and its revocation, is one of the biggest compliance issues addressed in the Order. The clarifications offered by the FCC will require companies to implement extremely detailed procedures and recordkeeping requirements, including for servicing transfers.

A business can avoid TCPA liability for certain calls if it can demonstrate it had consent from the "called party" to make the call. The Order clarified that "called party" does not mean the intended recipient of the call. So, even if a business intends in good faith to call a person from whom it has consent, the business could face liability if, for example, the number has been reassigned or the person who purportedly provided consent is not the subscriber or customary user of the phone. Thus, consent can come only from "the subscriber, i.e., the consumer assigned the telephone number dialed and billed for the call, or the non-subscriber customary user of a telephone number included in a family or business calling plan."

Let's take an example. Suppose my cell phone ➢

number is 555.444.3333, and that I gave you, my mortgage servicer, consent to call me on that line for debt collection calls. Then suppose I switch cell phone providers and get a new number without informing you, and my old cell phone provider assigns my old number to John Doe. If you call my old number and reach John Doe, you could face TCPA liability because you did not have consent to call the current subscriber, i.e., John Doe. This is a poignant concern because millions of cell phone numbers are reassigned each year. And some companies are already exploiting this requirement. If a telephone number had previously been assigned to, for example, a consumer who listed it on numerous credit applications and is receiving repeated debt collection calls, these companies will purposely purchase that number. Now, when those debt collection calls continue, those calls could expose the caller to significant liability because it does not have the consent of the current subscriber. Lawsuits have already been filed based on these scenarios.

**If you call my old number and reach John Doe, you could face TCPA liability because you did not have consent to call the current subscriber.**

What can you do to avoid this? First, the Order provides a very limited (and oftentimes unhelpful) exception. It states that a caller may avoid liability "for the first call to a wireless number following reassignment." The FCC reasoned that allowing this single call will give the caller an opportunity to learn the number has been reassigned. The problems with this exception are that (a) the single call may go unanswered or (b) it may be answered by the new subscriber who may not inform the caller the number has been reassigned. Nonetheless, if a business calls and learns a number has been reassigned, it needs to have in place detailed procedures and recordkeeping requirements to ensure that number is not called again.

Given the limited utility of the exemption, however, businesses may want to implement additional safeguards, including altering customer contracts and contracting with services that provide notices of reassigned wireless numbers. This especially true given that the burden of proof to demonstrate consent is on the caller and that regulatory agencies have been increasingly scrutinizing consent practices.

## WHO MAY REVOKE CONSENT?

The TCPA does not address whether consent can be revoked, and there had been industry disagreement over whether and, if so, how, consent could be revoked. The Order clarified that consent can be revoked in "any manner that clearly expresses a desire not to receive further messages." This includes, "for example, 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." The FCC specifically noted that a business "may not limit the manner in which revocation may occur."

This broad revocation right will require businesses to implement thorough training and recordkeeping procedures to verify that appropriate processes are in place to capture and honor revocations of consent. Although in the past some businesses have trained call center representatives to recognize and record any revocation, those trainings may now have to reach a wide range of employees that may come into contact with consumers, including employees at bill pay locations.

## EXEMPTIONS

The Order provides a few helpful exemptions. These exemptions, however, are very narrow and have very specific requirements for their use. It is therefore imperative that businesses have policies and procedures in place to identify and record when the exemptions apply.

First, "a one-time text sent in response to a consumer's request for information" is permitted so long as certain conditions are met. The text must (1) be requested by the consumer, (2) be a one-time message sent immediately in response to a specific consumer request, and (3) contain only the infor- ▷

mation requested by the consumer with no other marketing or advertising information.

Second, the Order grants a limited exemption from the TCPA for certain messages concerning time-sensitive financial and healthcare issues. For financial issues, the Order exempts calls and text messages concerning potential fraudulent activity or identify theft, possible data breaches, and money transfers. To fall within this exemption, the communications have to meet several conditions. They must (1) be placed only to the number provided by the consumer; (2) state the name and contact information of the financial institution; (3) be limited to the specific, urgent purpose without containing telemarking or debt collection information; (4) be limited to less than one minute or no more than 160 characters; (5) be no more than three messages per event over a three-day period for an affected account; and (6) contain appropriate opt-out options, and any opt-out request must be honored immediately.

## STATUS OF THE ORDER

Within days of the Order's effective date, a petition was filed to challenge some of the Order's findings. Other petitions have followed. Those challenges are underway and could have a significant impact on the validity of the Order.

In the meantime, however, TCPA litigation continues. Some courts have stayed cases to await the outcome of the challenges to the Order, but others have refused to do so. Courts have relied on and interpreted several of the Order's requirements in issuing judgments. So, businesses should strive for immediate compliance until the validity of the Order is ultimately determined. MCM

---

*Jeremy McLaughlin is an associate in the Consumer Financial Services group at K&L Gates LLP. His practice focuses on regulatory compliance and government enforcement for consumer financial products and services. He can be reached at Jeremy.McLaughlin@KLGates.com.*