Understanding TCPA Compliance Regulations

Among the updates is the inclusion of cellular phones, so that consumers could be protected from unwanted automated calls to a phone that could incur significant charges.

BY MARGARET L. WEIR, ESQ., CRCM

THINK BACK TO 1991. There was a phone in your parent's kitchen that hung on the wall, and likely had a cord half the length of a football field so you and your siblings could stretch it to talk in the next room. That phone rang constantly every night, with telemarketing calls. You probably did not own a mobile phone, but if you did, it was the size of a large brick or it was hard-wired into your car. Users were charged by the minute and there were no texting capabilities. The Telephone Consumer Protection Act ("TCPA") was passed that year to protect consumers from unwanted intrusions by telemarketers, and to create the "Do Not Call Registry." A lot has changed since 1991.

Since the TCPA's original passage, the Federal Communications Commission (the "Commission") has taken multiple actions implementing and interpreting the TCPA, and has issued numerous declaratory rulings clarifying specific aspects of the Act. Among the updates is the inclusion of cellular phones, so that consumers could be protected from unwanted automated calls to a phone that could incur significant charges. Protections include requiring callers to obtain express prior consent, which in some cases must be in writing. Those ignoring the rules do so with a bullseye on their back, not only from regulators but also from the plaintiff's bar. The law grants consumers a private right of action of up to $1,500 for *each* call. The exposure for violations includes potential FCC regulatory fines of over $16,000 per violation, per day, and possible state fines. Those running afoul of the regulators and consumers need also to consider the strong possibility of class action lawsuits.

In this article, we discuss the TCPA, the FCC rules under the TCPA, and the current litigation climate.

The TCPA in Brief

The TCPA generally restricts telemarketing calls and prohibits using an "autodialer" or "automatic telephone dialing system" ("ATDS") to make calls to a landline unless the call is for an "emergency purpose" or the caller has received prior consent, with some exceptions. There are strict restrictions regarding using an autodialer to call any cellular telephone service, or any service where the recipient of the call must pay for the call. Under the TCPA, it is "unlawful…to make any call, other than a call…*made with the prior express consent* of the called party, using any automatic telephone dialing system or an artificial or prerecorded voice…to any telephone number assigned to a…cellular telephone service." Therefore, calls and texts to cellular numbers will almost always require prior consent.

SHUTTERSTOCK/ WILLYAM BRADBERRY

What is an Autodialer?

The TCPA defines the term ATDS or "autodialer" to mean equipment which "has the capacity" (1) to store or produce telephone numbers to be called, using a random or sequential number generator; and (2) to dial such numbers. This system might connect the recipient to a human after placing the call, or it might contain an automated message. An "autodialer" also includes a "predictive dialer," which is equipment that is paired with software that dials a number, predicting when a sales associate will be available to take a call. The predictive dialer also has the capacity to store or produce numbers, and dial these numbers either at random, sequentially or from a database.

Under this broad autodialer definition, the FCC has determined that essentially all phone systems, other than rotary phones, have this "capacity," even where no such function has been enabled. The TCPA rules apply to text messages as well, as the FCC has determined a "text" is a "call" for purposes of this rule. Therefore the TCPA's reach is far and wide.

As with emergency communications, the requirements to identify the sender/caller, and the requirements for brevity and frequency, etc., remain.

Prior Consent

Consent is required for almost all text messages and calls to mobile numbers; the content and purpose of the message determines whether the consent must be in writing, or may be "express." The calls and texts where there is no consent necessary are those that are:

- Manually dialed without any prerecorded or automated message, for an "emergency" purpose;
- Those that are not for a business purpose and are from a non-profit and on the non-profit's behalf; and
- Those which are specifically exempted by a rule or declaration from the Commission.

For purposes of the TCPA, "emergency" communications under 47 C.F.R. § 64.1200, are those "made necessary in any situation affecting the health and safety of consumers." Calls and texts may not be made to those that appear on the FCC National Do Not Call List or an internal Do Not Call List. Those that are emergency in nature may not incur a charge. Generally, calls or texts must contain (within the call or text), a "mechanism for recipients to easily opt out of future calls" and texts. These communications must identify the sender/caller and are limited to three within any three-day period, per event, with phone messages being under one minute and text messages no more than 160 characters.

Informational Calls and Texts

Informational calls and texts require prior express consent, but do not require consent in writing. These calls have the same technical requirements as stated above. Examples of informational calls would be a call to let a customer know their checks are ready for pickup at a branch, or a call to let the customer know their certificate of deposit is maturing. Again, be careful that you do not add sales messages about how they could rollover that CD, because then it is marketing, and you would need written consent, as discussed below. Debt collection calls would come under informational as long as there is no marketing crossover—however, consent must be given in connection to the underlying debt—for example, by the customer on their loan application. There is currently some debate about exemptions where the call is to collect federal government debts, which is beyond the scope of this article. For the time being, it is best to err on the side of caution with these too, and obtain prior express consent.

Express Consent

It is important to note that the FCC has determined that a customer has given express consent when the customer knowingly releases their phone number. An example of this would include a customer listing their cellular number on an account, loan application or other official documentation. The burden to show the caller had consent is always on the caller. Thus, a financial institution would be wise to note how they obtained a customer's phone number, as well as if the number is currently a mobile number and as discussed below, notation of whether the phone number remains valid. Understand also that where you have a landline number, the number can be "ported" or converted into a cell number, thus it would be wise to treat all calls as if they were to a mobile number.

Written Consent—Telemarketing Calls and Texts

Financial institutions that initiate telemarketing calls using an autodialer, and using artificial voices or prerecorded messages, are required to obtain express written consent for telemarketing calls (including text messages). Such calls and texts must comply with the requirements stated above.

Calls that are "telemarketing" in nature, include any calls during which there is encouragement to purchase of investments, property, goods, or services. For these calls, prior written consent must contain the following:

- An identification of the entity to whom consent is being provided, and the customer's phone number which will be used for the communications; and
- A disclosure, which must also be clear and conspicuous informing the person signing that by executing the agreement, they authorize the seller to deliver telemarketing calls using an automatic dialing system, or an artificial or prerecorded voice. The disclosure must also include a statement that the person is not required to sign the agreement, or agree to enter into such an agreement, as a condition of purchasing any property, goods or service.

The signature may be electronic or digital if such signature complies with E-Sign. Once prior consent is granted, there are restrictions to the content and frequency of messages that are the same as stated above for other calls.

Settlement amounts over the past several years for financial companies

Name of Institution	Amount of Settlement
Capital One Bank, N.A.	$75 Million
HSBC Bank Nevada, N.A	$40 Million
Bank of America Corp.	$32 Million
Wells Fargo Bank, N.A.	$30.4 Million
Wells Fargo Bank, N.A.	$16.3 Million
J.P. Morgan Chase Bank, N.A.	$10.2 Million
American Express Co.	$9.25 Million
The Western Union Company	$8.5 Million
Comenity Bank	$8.5 Million
Navy Federal Credit Union	$2.75 Million

Prior Consent Exempted for Certain Financial Institution Communications—The 2015 Omnibus Declaratory Ruling and Order:

In the 2015 Omnibus Declaratory Ruling and Order ("Order"), the Commission found that certain calls/texts from financial institutions are "intended to address exigent circumstances in which a quick, timely communication with a consumer could present considerable consumer harms from occurring or…could help quickly mitigate the extent of harm that will occur." Thus, the Commission exempted from the prior consent requirement, certain types of calls and texts, made to a number provided by the customer. Those types of calls are those that are:

- Fraud/suspicious activity or identity theft alerts, as long as they don't also contain marketing messages;
- Steps consumers can take to prevent or remedy harm caused by data security breaches; and
- Actions needed to arrange for receipt of pending money transfers.

As with emergency communications, the requirements to identify the sender/caller, and the requirements for brevity and frequency, etc., remain. However, the opt-out may be specific in terms of one of the exempted categories, so that recipients are opting out of one category, but not necessarily all messages. An example would be an opt-out option for only fraud alerts, where the recipient would still receive data security and money transfer calls and texts, unless they opted out of those separately.

The Commission cautioned: "…these calls may not contain telemarketing, cross-marketing, solicitation, debt collection, or advertising content of any kind…" therefore, be careful that you do not co-mingle any of these exempt, "informational" or "emergency" communications with telemarketing—you would need written consent if you cross that line!

An example would be an exempted call to a customer whose account may have been compromised. It would be improper during that call to mention any services that the recipient could obtain to mitigate identity theft. Where the caller mentions such a product or service, it crosses into "telemarketing" territory, where such written consent would be required.

Consent Revocation

Once consent is obtained, the customer must always have a means to "opt-out." A customer's request to stop texts or calls must be recognized immediately, and the regulations do not allow any restriction on how a customer may convey their desire to stop calls and/or text messages, only stating that a person may make the request in any "reasonable" manner. This means, practically, that a customer could tell a bank teller that they wish to be removed from calls and texts, and that would be deemed notice under the rules. A customer could also email virtually anyone in the institution, and this would constitute notice. Once notice to opt-out is received, the institution must recognize the opt-out as soon as possible. As discussed below, the financial institution is exposed each day after the notice, if the opt-out is not processed timely.

Reassigned Phone Numbers

One of the most significant rulings of the FCC in their 2015 Order, addresses the reassignment of cellular phone numbers. Cellular numbers are routinely re-assigned after a customer switches to a new carrier, or closes their mobile account. Currently, there is no reliable way for a business to determine whether or not the number remains associated with their customer, except by calling that number and checking with the customer on a regular basis to verify the customer's information. The caller can only call or text once to a reassigned number before violating the TCPA. This means, the caller or message sender may not have constructive knowledge that the number has been reassigned until later. Unfortunately, this does not matter and a violation occurs regardless of "knowledge."

The Order suggested the financial institution might take the following steps to attempt to learn that a cellular number has been disconnected, including:

- Periodically sending requests to the communication recipient to update their contact information;
- Implementing controls that require customer service representatives and contact center employees to ask for updated information; and
- Implementing controls to keep track of calls when the caller notices a new name in the recording, or when the number indicates it has been disconnected.

Financial institutions must understand their systems and sales and notification programs and have strong policies, procedures, training and record-keeping to battle any challenges, and understand that even then, there may be exposure to plaintiff attorneys looking for settlements.

Litigation and Regulatory Actions

In addition to actions brought by the Commission and state attorneys general, the TCPA allows private causes of action. Private causes of action can result in between $500 and $1,500 in statutory damages for each violation (call or text), as well as injunctive relief. Keep in mind that the plaintiff in each case does not have to prove any actual harm. Commission fines can be more than $16,000 per violation, per day, in addition to potential state fines. Violators of the TCPA are exposed to class action suits, as there is no ceiling to the amount that can be assessed in total.

According to the U.S. Chamber Institute for Legal Reform (the "Institute") 2017 report "TCPA Litigation Sprawl: A Study of the Sources and Targets of Recent TCPA Litigation," more than 3,121 TCPA suits were filed between August 1, 2015 and the end of 2016. This shows only those filed electronically, and indicates an increase of 46%, after the 2015 Order. For the same period prior to the Order, there were approximately 2,127 cases listing a claim under the TCPA as reported by the Institute.

The analysis of the Institute further shows that it is not spam telemarketers/texters that are involved in the lawsuits, but rather communications such as flu shot reminders, customer transaction calls, delivery alerts and customer satisfaction surveys, stating, "…the lawsuits examined…seek aggregated statutory damages from legitimate American companies not engaged in the kinds of cold-call telemarketing the TCPA was designed to limit…the sprawl of TCPA litigation illustrates the serious problem that occurs when uncapped statutory damages and a technologically-outdated statute work together to over-incentivize litigation."

TCPA lawsuits have been filed in almost every type of industry, with the Institute reporting the hardest hit "by far" being brought against banks and other financial services entities. More than 36% of those examined were within the financial services sector, not including debt collection, which was an additional 18.1% of litigation for the period. Each of the top twenty defendants was named in at least 17 TCPA cases in the sample group, and together they faced 601 class action and individual TCPA lawsuits within the 17-month 2015–2016 time period. The Institute also found myriad cases brought against affiliated companies. Examples would be those brought against most Citi-related entities during the period—where Citibank, Inc., Citigroup, or Citimorgage together had 77 suits filed against them in the period.

More than one-third of the total cases filed were nationwide class actions. Of those class actions, statutory damages sought ranged from the millions to billions of dollars. This bullies companies into large settlements rather than accumulated court costs to prove innocence, and the system churns on, encouraging even more litigation.

The actions have spawned a cottage industry of litigation firms, with only 44 law firms filing the majority of actions, where 2 firms filed more than 200 TCPA litigation actions each, in the sample. Remember the ATM litigation boom of a few years ago? That pales in comparison. The litigation industry has also resulted in "professional plaintiffs" where the Institute finds individuals who are repeat litigants for every text and phone call they have received, going back multiple years. Even where no autodialer is in evidence, cases are proceeding through the discovery phase as discussed in the Institute's paper. This is the case where the defendant may be found innocent of the violations, but will incur sometimes debilitating court costs to prove the innocence. Most often, it is advantageous to settle, even where innocent.

Why the increase in TCPA litigation? There are a number of reasons, but perhaps the number one reason is the increase in cellular phone use overall, and in particular the use as the plaintiff's only phone. Consider that as of 2016 there were 349.9 million wireless connections in the United States. Forty-nine percent of all U.S. households were "wireless-only" (as reported by the wireless industry trade association, CTIA), and 261.9 million of those total wireless connections were smartphones.

Keep in mind that there are only 323 million people in the United States, with approximately 252 million of those over the age of 18, per the Census Bureau. This means every U.S. adult and some children likely have a smartphone capable of receiving calls and texts. It is not a leap to assume financial institutions are contacting customers on wireless numbers ripe for litigation exposure.

Types of Litigation

The following are types of TCPA litigation that we are seeing the most today:

- How and if consent was obtained and the scope of consent;
- Where there is consent, whether or not consent was revoked and whether or not the entity contacted the consumer after revocation;

- Issues related to how consent was revoked, and what phrases must be recognized (STOP; END; CANCEL; UNSUBSCRIBE and QUIT);
- Challenges to the type/content of particular text messages;
- Issues related to shared liability between entities for whom the message is sent, and text platform providers;
- Issues regarding how mobile numbers were obtained and disclosure adequacy; and
- Reassigned/Recycled number litigation.

Conclusion

Financial institutions must be aware of the risks associated with the TCPA, and understand that compliance is not necessarily a safeguard against the filing of a suit. Financial institutions must understand their systems and sales and notification programs, and they must have strong policies, procedures, training and record-keeping to battle any challenges. In addition, they must understand that even then, there may be exposure to plaintiff attorneys looking for settlements. The best defense therefore, is a great program that includes all levels and technologies within the institution, and a heightened awareness by every employee who may have contact with a customer. ■

ABOUT THE AUTHOR

MARGARET "MAGGIE" WEIR, ESQ., CRCM, is an experienced regulatory compliance and legal professional with more than 25 years of experience in leadership roles with multiple financial institutions and consulting groups. Maggie is a practicing attorney and adjunct faculty for the J.D. and LL.M. programs at Boston University School of Law. She regularly teaches programs on a variety of legal and compliance topics for the Massachusetts Bankers Association and is faculty for the American Bankers Association National Compliance School. Maggie can be reached at **magweirlaw@gmail.com**.

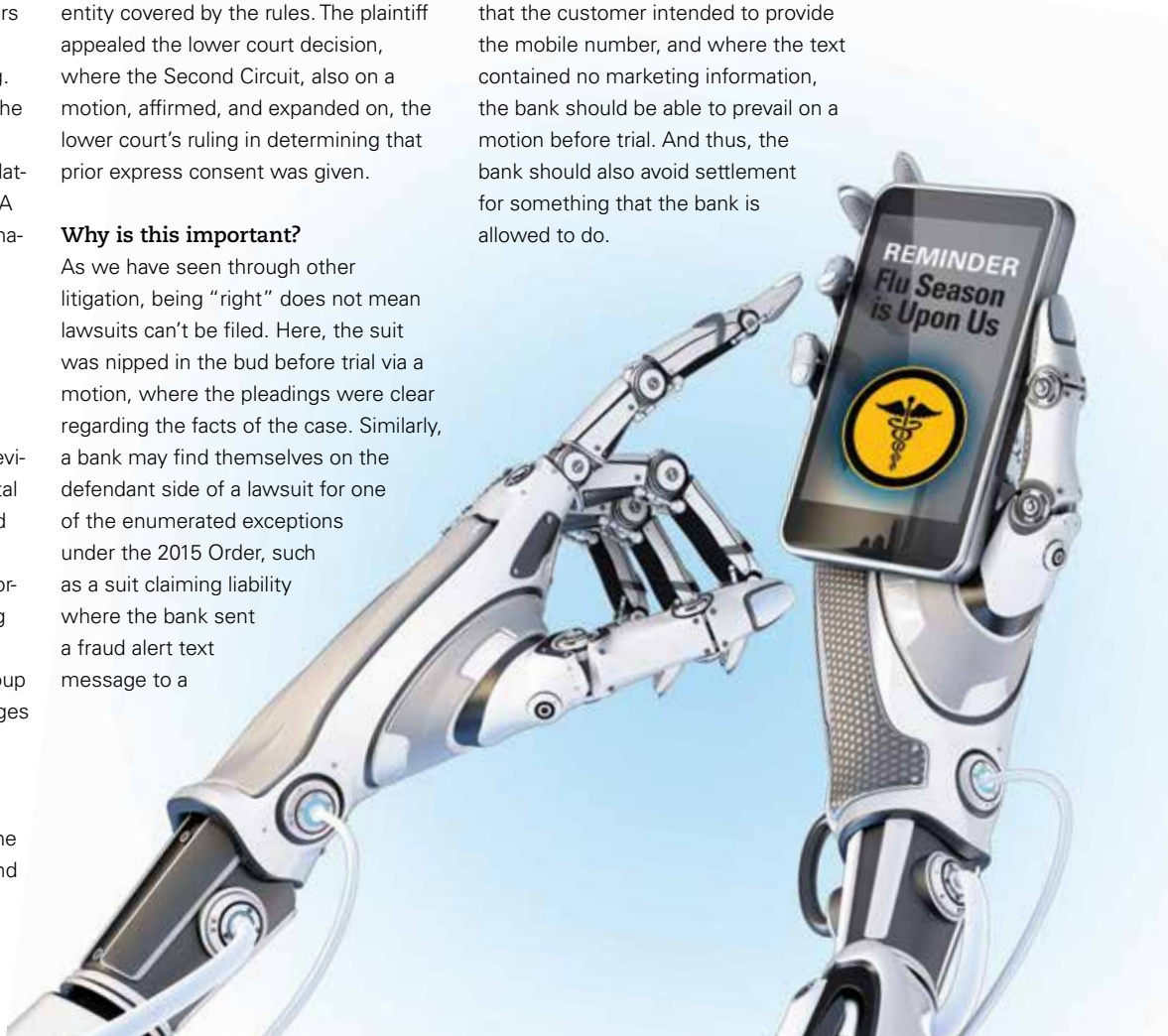
Healthcare "Phones In" a Win!

Similar to the exceptions formed for banks under the 2015 Order, there are exceptions for health care providers to send "health care messages" that came about through a 2012 FCC ruling. Recently the Second Circuit ruled on the scope of that rule. The Second Circuit ruled that a reminder text message relating to flu shots did not violate the TCPA where the patient had given his information, including the mobile number, for treatment purposes.

In the underlying case, the plaintiff brought a class action alleging that a hospital group violated the TCPA by sending a reminder text to patients to get their flu shots. The plaintiff had previously visited a subsidiary of the hospital group for an exam, and had completed new patient forms at that time, which included consent to use his health information for specific purposes, including "for payment, treatment and hospital operations purposes." The hospital group hired a third party to send text messages on their behalf, and in 2014 they sent a single reminder text to the plaintiff regarding flu season. The lower court ruled on a motion for a judgment on the pleadings for the defendants, and found that the message was exempted from written consent because it delivered a "health care message" on behalf of an entity covered by the rules. The plaintiff appealed the lower court decision, where the Second Circuit, also on a motion, affirmed, and expanded on, the lower court's ruling in determining that prior express consent was given.

Why is this important?

As we have seen through other litigation, being "right" does not mean lawsuits can't be filed. Here, the suit was nipped in the bud before trial via a motion, where the pleadings were clear regarding the facts of the case. Similarly, a bank may find themselves on the defendant side of a lawsuit for one of the enumerated exceptions under the 2015 Order, such as a suit claiming liability where the bank sent a fraud alert text message to a customer who had clearly and intentionally given the bank their number. In such a case, where the bank is able to show that the customer intended to provide the mobile number, and where the text contained no marketing information, the bank should be able to prevail on a motion before trial. And thus, the bank should also avoid settlement for something that the bank is allowed to do.



SHUTTERSTOCK/ WILLYAM BRADBERRY