AMERICAN MARKETER

Business at its best

COLUMNS

What your service provider is not telling you about new TCPA rules for SMS/MMS marketing

October 17, 2013

By Michael Ahearn

We have all seen the Armageddon dates come and go with a chuckle. Millennial computer clocks. Mayan calendars. Oct. 16, 2013.

Wait, why Oct. 16? If you do not know already, on Oct. 16, 2013 new Federal Communication Commission rules under the Telephone and Consumer Protection Act (TCPA) went into effect.

Without an action plan and proper planning, this date could indeed become Judgment Day for your existing SMS/MMS programs and opt-in databases.

October revolution

If your existing SMS/MMS database members did not provide prior express written consent to new TCPA consent requirements before Oct. 16, then any SMS/MMS marketing messages sent to them after Oct. 16 may make you an unwitting illegal telemarketer, liable to fines and exposed to class action lawsuits.

This applies for all new opt-ins as well, and requires new consent language to be clearly and conspicuously displayed in all media calls to action to opt-in. Pretty serious stuff.

When you do the math for fines of $500 to $1,500 for every non-compliant message sent after Oct. 16, and multiply that by the mobile opt-in membership of big brand databases, we are talking substantial exposure potentially in the tens to hundreds of millions of dollars.

First a necessary disclaimer: what you read here should not be taken as legal advice, and may not be appropriate for your particular situation. You should not act or rely on any information discussed here without seeking the advice of an attorney.

Secondly, there are other voices in the industry who are taking a "business as usual" stance in regards to the new TCPA rules and deadline.

Indeed, their position relies on the view that SMS marketing messaging is excluded from the new TCPA rules because the new rules are not intended to apply to existing mobile databases, and/or they are not delivered by an "automated telephone dialing system" as regulated by the FCC and TCPA.

Many of the same voices are leading the charge, to their credit, to get mobile industry organizations to petition the

FCC for clarification on these aspects of the rules.

But this does not change the fact the rules are in effect now as of Oct. 16, with the potential exposure to any lawyer seeking to exploit non-compliance to file class action lawsuits.

Class of its own

Wireless carrier-compliance requirements just add to the confusion. There are already "compliant opt-in" best practices required by carriers and promoted by the CTIA and Mobile Marketing Association.

Many companies already employ "double opt-in" with consumer consent replies as part of an opt-in message flow.

There are people in the industry today who state that these carrier regulations and best practices will satisfy TCPA rules.

Nothing could be further from the truth, unless these best practices and requirements are updated.

If you adopt this "business as usual" or "I'm already compliant with the carriers" stance, you may be subjecting your company to significant legal exposure.

What is key here is that existing carrier regulations and opt-in mechanics have not yet been adapted to the new TCPA consent requirements.

Furthermore, carrier requirements are based on carrier interpretations of applicable law and may or may not be consistent with the way courts apply the TCPA.

So it may not be wise to outsource your legal compliance and risk mitigation decisions to industry groups during times of such dramatic change.

While one may argue and petition whether existing SMS/MMS databases should fall under FCC/TCPA rule sets, or how TCPA "autodialer" definitions should or should not apply to SMS/MMS marketing technology, the critical question your company must ask is what position and actions you will take now to address potential legal challenges to your TCPA compliance vis vis the Oct. 16 rules.

Many legal teams of large brands, both our customers and non-customers, have come to the conclusion that they are potentially exposed to, and therefore must comply with, the new Oct. 16 TCPA rules.

The proof is the wave of messaging to existing SMS/MMS databases we have seen asking for consumer re-opt-in using TCPA compliant written consent, either via Web check box, SMS/MMS response to TCPA disclaimer language, or both.

We are also seeing the new TCPA compliance language displayed on Web sites, social pages and all other media where opt-in calls to action are promoted for new opt-ins. "Better safe than sorry" seems to be the strategy many major brands and companies are taking.

Taking priority

So what is specifically different about the new TCPA compliance requirements that are not understood or accepted by the "business as usual" view?

The new TCPA rules involve a very technical, specific definition of what type of consent can satisfy the new "prior written consent" requirement for SMS/MMS marketing messaging.

"Prior written consent" requires three things:

1. A signature in any manner that complies with e-sign or state law

2. A clear and conspicuous disclosure that, by signing, the person authorizes the seller to deliver marketing text messages using an automatic telephone dialing system to the number provided.

3. A clear and conspicuous disclosure that the person is not required to sign the agreement as a condition of purchasing any property, goods or services.

To be clear, if a consumer has not provided consent in the manner described in the rule (i.e. with the specified disclosures) then you do not have "prior express written consent" as defined in the rule.

And if you do not have "prior express written consent" from a customer, then the rule appears to state that you cannot send them marketing text messages after Oct. 16, 2013.

The net effect is brands conscious of the new rules have deployed TCPA compliance programs to make their existing database members TCPA compliant, and ensure all new opt-ins are TCPA compliant as well.

Before the Oct. 16 deadline, brands sent messages to their mobile databases via SMS/MMS to get this written consent, commonly with a message containing the required disclaimer and a request for the consumer to reply

"YES" to capture the written consent.

The key here is that if the new rules do apply to existing databases, and if a re-opt-in message is a marketing message, then you would no longer be able to deploy this tactic after the Oct. 16 deadline, since you would be sending a marketing message to a non-compliant database member. Seems like something from Catch-22, but there it is.

Long and short of it

In a nutshell, what does this mean post-Oct. 16, and what can you do to get your database back in compliance?

Here is what went into effect since Oct. 16:

1. All new opt-ins must comply with prior express written consent to the new TCPA rules, which needs to be captured and made available if audited.

The required signature may be obtained in any manner that complies with applicable state or federal law including via email, Web site form, text message, telephone key press or voice recording.

2. Depending on whether the new rules are intended or not intended to apply to existing databases and your willingness to take the risk that they do, you may no longer be able to send SMS/MMS marketing messages to existing database members if you do not have their prior written consent as stipulated in TCPA rules.

If you decide that you are going to require TCPA-compliant re-opt-in, then database members without recorded written TCPA-compliant consent become "inactive" members, who can only be "re-activated" for messaging when you have their written consent or when a final determination is made by the FCC that the rules do not apply to existing SMS/MMS databases.

The wheels of government normally grind slowly. I would not hold my breath for quick clarifications.

The present government shutdown could be creating a backlog at the FCC, further delaying the speed of response on this issue. Also, there is the clear possibility that the mobile industry petitions could be denied altogether.

Don't shelve it

Which brings up the complication that your SMS database members have a shelf life.

Carrier regulations and general marketing best practices require that you send messages to opt-in members regularly. You cannot wait forever and send a message out of the blue after six months when you finally get their TCPA compliance.

Compliant re-opt-in needs to happen as soon as possible, so you can continue to send messages to your mobile database. Best practice is to send a message to opt-in group members at least once a month.

So how do you get this consent if you cannot send them an SMS asking for it?

That is a great subject for another article, but in short you can point them to Web-based TCPA-compliant forms via email, social pages, mobile and PC Web pages, or via new mobile calls to action in any media TCPA-compliant, of course that makes them a compliant member.

Good tactics that properly incentivize the consumer to participate such as coupons, sweepstakes, instant wins and the like can be offered.

The key here is that you consider whether or not to make the incentive a reward for re-opting inconsult with your lawyers on whether this is a good idea as there is more legal grey area here.

REGARDLESS OF how you offer the incentive to join the program, make sure the opt-in mechanics are TCPA-compliant.

Major brands are taking steps to shore up the integrity of their existing database, and make the necessary disclaimer changes on their marketing materials, text messages and Web sites.

Hopefully your mobile service provider has provided you with accurate advice, and you are working on your present and ongoing strategy to deal with all aspects of the new TCPA rules.

Michael Ahearn is San Francisco-based vice president of customer development and marketing at Archer, a provider of mobile engagement solutions and services, including mobile database compliance programs. Reach him at michael.ahearn@archermobile.com.