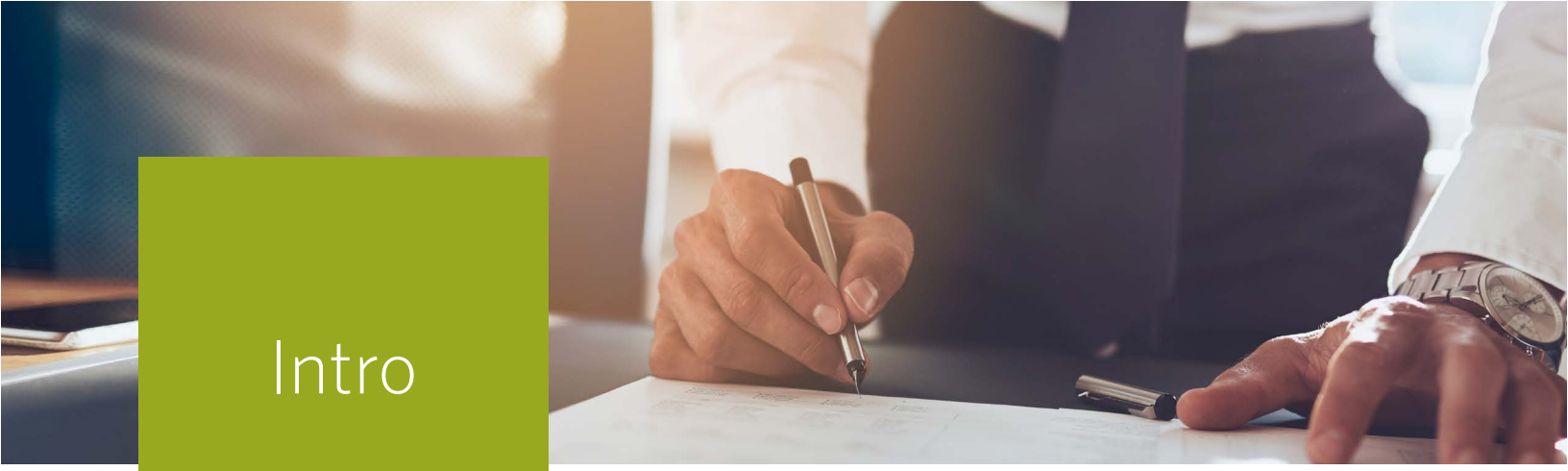
ActiveProspect | KMT KLEIN MOYNIHAN TURCO LLP

CONSENT TO CALL?

Internet Leads & the Telephone Consumer Protection Act



Intro

On October 16, 2013, new FCC regulations will go into effect that introduce the requirement of prior express written consent for certain types of commercial phone calls and text messages to consumers. Among other things, the new rules require that marketers have prior express written consent to autodial or send pre-recorded messages to cell phones. The rules, which put the burden of proof for compliance on the marketer/caller, come with stiff penalties ($500.00 - $1,500.00 per call/text) and will open the door for numerous consumer class action lawsuits.

The new Telephone Consumer Protection Act (TCPA) rules will have broad implications for three reasons. First, many marketers that make outbound calls to consumers utilize call centers. These call centers typically use “autodialing” software to make the calling process more effcient. Second, a growing percentage of U.S. households exclusively rely on wireless phones. As of June 2012, 35.8% of U.S. households were wireless only[1]. Third, consumers can bring private lawsuits or initiate class action lawsuits against marketers that violate the regulations. This combination of high numbers of autodialed calls, coupled with increasingly exclusive reliance on mobile phones and sti penalties for non-compliance, make these changes significant.

This paper is focused on Internet leads, also known as web leads or inquiries. An Internet lead is a consumer inquiry generated when a consumer fills out a form on a website requesting to be contacted by a business (marketer). Internet leads are often purchased by marketers on a cost per lead basis. Companies that buy and sell Internet leads are part of the Online Lead Generation Industry, a $1.7 billion industry in 2012[2].

This is a two part whitepaper, provided by the law firm of Klein Moynihan Turco LLP (KMT) and ActiveProspect, a marketing Software-as-a-Service (SaaS) provider. Part 1, written by KMT, provides a background on the legal aspects of the new TCPA regulations as they pertain to Internet leads. Part 2, provided by ActiveProspect, highlights a simple and comprehensive solution to verify and store proof of consent for Internet leads for purposes of compliance with the new regulations.

---

1 Center for Disease Control National Health Interview Survey

2 IAB Internet Advertising Revenue Report 2012 full year results April 2013

PART 1:

TCPA Rules & Steps for Compliance

Written by Klein Moynihan Turco LLP

Background on the TCPA

The TCPA was passed into law in 1991 and granted the Federal Communications Commission (FCC) the power to issue rules and regulations to govern the expanding telemarketing industry. Among other things, the TCPA allows individuals to file lawsuits and collect damages for receiving certain types of unsolicited telemarketing calls, text messages, faxes, pre-recorded calls and autodialed calls. The TCPA applies to both voice and short message service (SMS) text messages, if they are transmitted for telemarketing purposes – with limited exceptions (e.g., messages sent for emergency purposes). "Telemarketing" calls include those made by marketers that offer or market products/services to consumers. Purely informational calls and calls for non-commercial purposes are exempt from the TCPA amendments discussed below.

Autodialers

An autodialed call is a phone call, involving a live person or pre-recorded message, that is placed using an "autodialer," or automatic telephone dialing system, that has the capacity to produce, store and call telephone numbers using a random or sequential number generator. The autodialed call definition should be broadly construed in an effort to avoid unwanted litigation and regulatory action. For instance, if you are utilizing any type of call center software as part of your telemarketing operations, you may be using an autodialer within the FCC's definition. If you are unsure, we recommend that you consult with an attorney who has expertise in telemarketing law.

New TCPA Rules

In a Report and Order approved on February 15, 2012, the FCC adopted additional protections for consumers concerning unwanted autodialed calls/texts and/or pre-recorded messages. Two of these new rules are scheduled to go into effect very shortly.

First, beginning October 16, 2013, prior express written consent will be required for all autodialed and/or pre-recorded calls/texts sent/made to cell phones and pre-recorded calls made to residential landlines for marketing purposes. Compliance with the E-SIGN Act satisfies this requirement, meaning that electronic or digital forms of signature are acceptable (i.e., agreements obtained via email, website form, text message, telephone keypress or voice recording). Under the new rule, consumer consent must be unambiguous, meaning that the consumer must receive a "clear and conspicuous disclosure" that he/she will receive future calls that deliver autodialed and/or pre-recorded telemarketing messages on behalf of a specific marketer; that his/her consent is not a condition of purchase; and he/she must designate a phone number at which to be reached (which should not be pre-populated by the marketer in an online form). Limited exceptions apply to this requirement, such as calls/texts from the consumer's cellular carrier, debt collectors, informational notices and healthcare-related calls.

Sample Website Consent Language:

> ☐ I hereby consent to receive autodialed and/or pre-recorded telemarketing calls from or on behalf of [Marketer's Legal Name] at the telephone number provided above, including my wireless number, if applicable. I understand that consent is not a condition of purchase.

If a dispute concerning consent arises, the marketer bears the burden of proof to demonstrate that a clear disclosure was provided and that the consumer unambiguously consented to receive telemarketing calls to the number he/she specifically provided. It is a best practice for marketers to maintain each consumer's written consent for five (5) years. Evidence of Internet-provided written consent includes, but is not limited to, website pages that contain consumer consent language and fields, an associated screenshot of the consent webpage as seen by the consumer where the phone number was inputted, and a complete data record submitted by the consumer (with time and date stamp), together with the consumer's computer IP address.

Second, beginning October 16, 2013, the "established business relationship" exemption for pre-recorded telemarketing calls to residential landlines will be eliminated. In the past, marketers could rely on an established business relationship (such as a previous purchase) to circumvent the need to obtain a consumer's consent to receive pre-recorded telemarketing calls. That exception to the consent requirement will no longer exist after this year. Marketers will have to obtain written consumer consent, as outlined above, even if they previously had a business relationship with the consumer.

Penalties

The TCPA provides for either actual damages or statutory damages ranging from $500.00 to $1,500.00 per unsolicited call/message. In determining the final amount of statutory damages to award, courts analyze whether the defendant "willfully" or "knowingly" violated the TCPA. Considering that telemarketing campaigns often involve thousands to, in some cases, millions, of calls/text messages, potential damages under the TCPA may escalate very quickly.

Recent TCPA Cases

TCPA cases have been leading legal news with almost weekly multi-million dollar class-action settlements. By various accounts, TCPA filings are up 40-60% in 2013, when compared to the same period in 2012. For instance, Steve Madden, Ltd., an international shoe retailer, was accused of sending more than 200,000 text messages to consumers, but claimed that consumers had consented to receive the messages by providing their cell phone numbers while visiting Steve Madden's stores and website. The court found that clear and conspicuous consent had not been adequately proved and Steve Madden ultimately settled the case out of court for more than $10 million.

TCPA CASES:

TCPA filings are up 40-60% in 2013, when compared to the same period in 2012.

PART 2:

TCPA Compliance Solution

Written by ActiveProspect, Inc.

Obtaining Consent is the Key to Compliance

The purpose of the TCPA is to limit the number of unwanted telemarketing solicitations. While these regulations may reduce unwanted calls to consumers, they also create administrative headaches for responsible businesses trying to communicate with their existing and potential customers. For a TCPA compliance solution to be effective for the long-term, it must be a solution that works within both the spirit and the letter of the law. As such, obtaining proper consent from consumers is the most effective way to comply with the new regulations and avoid costly litigation.

One of the most significant TCPA rules going into effect is the requirement to obtain prior express written consent for auto-dialed calls to cell phones. One compliance approach would be to avoid using auto-dialers for calls to cell phones. However, with authoritative proof of prior express written consent, there is no need to determine the type of phone number provided or change the type of system used to dial the number. Therefore, the simplest solution is to get the proper consent for all leads instead of relying on work-around solutions that require different calling methods for dierent types of phone numbers.

When a consumer submits his/her phone number on a website requesting to be called, there is implied consent. However, once the new TCPA rules take effect on October 16, 2013, marketers must prove prior express written consent by adding the proper legal disclosures on the forms, outlined in Part 1 of this paper by KMT, and retaining evidence that consent was provided. When marketers buy Internet leads, they expect that those leads have requested to be contacted and provided consent, but this is not always the case. Independently verifying and storing that consent is not only good business, it is also the simplest way to shield yourself from potential liability. But more importantly, why buy an Internet lead for a consumer who doesn't want to be contacted?

PROOF OF CONSENT: THE TRUSTEDFORM SOLUTION

Once the proper disclosures are added to web forms where leads are collected, marketers must reliably capture and store evidence that proper consent was obtained for all Internet leads. Creating a reliable, consistent system for recording proper consent that will hold up under legal scrutiny presents a significant challenge for marketers. ActiveProspect has solved this problem with its patent-pending TrustedForm lead certification solution. It is a simple way to achieve compliance, avoid business disruptions and maintain the ability to communicate directly with consumers.

How it works

Once the proper disclosures are added to web forms where leads are collected, marketers must reliably capture and store evidence that proper consent was obtained for all Internet leads. Creating a reliable, consistent system for recording proper consent that will hold up under legal scrutiny presents a significant challenge for marketers. ActiveProspect has solved this problem with its patent-pending TrustedForm lead certification solution. It is a simple way to achieve compliance, avoid business disruptions and maintain the ability to communicate directly with consumers.

TrustedForm issues Certificates of Authenticity that independently verify the origin of Internet leads. It works by adding the TrustedForm script to the web page where leads are collected. The script then issues a TrustedForm Certificate for every lead generated on the site. This Certificate is a virtual document that provides critical evidence of prior express written consent for each lead. Each TrustedForm Certificate is accessed by a unique URL so that it can be easily referenced as one additional field with each lead record in your database. Since it is presented as a complete authoritative document, it can be easily printed or passed along to the appropriate parties as needed. TrustedForm provides a centralized repository of authoritative evidence of consent. With authoritative proof of prior express written consent, there is no need to determine the type of phone number provided or change the type of system used to dial the number.

- Date and time of the consumer's visit to the web page;
- URL where the consumer completed the form. If the form is in an iframe, it also captures the parent URL where the form is framed;
- The IP address, browser and operating system of the visitor who submitted the form;
- Real-time screenshot of exactly what the consumer saw when he/she visited the form page This is important for a visual inspection of what the consumer saw and indicates whether data such as the phone number and consent check box was pre-populated on the web form; and
- A complete copy of the HTML and images of the web page where the consumer filled out his/her information. This is important to be able to interact with the web page as it existed at that point in time and allows for real-time page scanning for disclosure language.

TrustedForm Certificates independently collect the following information:
A TrustedForm Certificate, in conjunction with a record of all the lead data that was submitted by the consumer, creates authoritative evidence of whether consent was properly obtained. In addition, TrustedForm contains other features that are important for verifying consent compliance:

Lead Fingerprinting technology is embedded in every TrustedForm Certificate. This feature solidifies evidence of consent by allowing a marketer to independently verify that the phone number that was received with the lead data was the same phone number that was actually input on the web form by the consumer. None of the consumer's personally identifiable information is captured by TrustedForm as part of this process and the verification takes place in real-time prior to the marketer calling the consumer.

Real-Time Page Scanning verifies the presence of required consent and disclosures, and/or absence of restricted content, all in real-time. This allows marketers to immediately verify

ADDRESSING THE CHALLENGES OF VERIFYING AND STORING EVIDENCE OF CONSENT

Challenge: Must have proof of consent for every lead.

Any consumer contacted can bring a suit against a business for non-compliance with the regulations. Therefore, proof of consent must be stored for every single lead received in a marketing database. Businesses must be able to provide proof of consent for each individual by proving that the consumer in question was presented with the proper consent language and verifying the phone number submitted on the form.

Solution: Store a TrustedForm Certificate for every lead.

Challenge: Proof of consent should be stored for 5 years.

Because of the statute of limitations to bring action under the TCPA, proof of consent should be stored for 5 years.

Solution: TrustedForm allows Certificates to be stored indefinitely on secured servers.

Challenge: URLs are insufficient evidence as websites constantly change.

Consider how many times a website may change over five years. Furthermore, many of the sites where leads are collected are dynamic websites (content changes for each individual visitor). Compliance requires a business to prove exactly what the consumer saw when he/she agreed to submit their phone number. A URL will not meet this regulatory requirement. A sufficient record can be achieved with a real-time screenshot or page snapshot.

Solution: In addition to the URL, TrustedForm captures a real-time screenshot and page snapshot of exactly what the consumer saw when he/she visited the web page.

Challenge: Obtaining reliable proof from 3rd party lead vendors.

For companies that purchase Internet leads from lead vendors, the burden of proof is on the lead buyer. Marketers must have proof that the lead purchased provided prior express written consent for their specific business to call the lead using autodialer technology and/or pre-recorded messages. It can be difficult to receive reliable information on the origin of Internet leads since they are commonly brokered between multiple layers of lead vendor relationships. Even reputable vendors may be purchasing leads from sources of questionable reliability. To further complicate matters, vendor relationships may be terminated or vendors could cease operations during the recommended 5 year storage window.

Solution: TrustedForm independently captures reliable proof directly from where the lead was originally collected.

Challenge: Must verify consent prior to dialing.

If using an autodialer (for cell phones) or pre-recorded messages (for cell phones and landlines), proof of express prior written consent must be verified prior to calling the lead. Generally lead buyers want to contact leads as quickly as possible, so adding a step of manual consent verification could slow down the sales process.

Solution: The Real-Time Page Scanning feature verifies the presence of the proper disclosures in real-time before dialing the lead.

Challenge: Verify disclosures comply with the law.

There are a variety of legal guidelines to be met for how consent is obtained. For example, disclosures must be presented to the consumer in a “clear and conspicuous” manner, the phone number must not be pre-populated on the form and the consent check box, if applicable, must not be pre-checked.

Solution: In addition to real-time page scanning, TrustedForm allows for visual review of exactly what the consumer saw including whether fields were pre-populated.

Challenge: Need for independent authoritative reliable evidence.

In a legal dispute or customer complaint, it is the word of one party against the other. The consumer will claim that he/she did not give consent while the lead buyer will argue that proper consent was obtained. Therefore, it is important to have authoritative evidence that is captured and stored by an independent third party because the burden of proof of compliance with the TCPA ultimately rests with the marketer. This evidence needs to be in a form that can be clearly presented as proof to the judicial fact-finder or individual consumer.

Solution: TrustedForm is the proven solution for independently verifying consumer consent. TrustedForm Certificates provide a simple authoritative document for each lead, as well as video replay of the interaction.

Conclusion

Complying with TCPA regulations - as they relate to Internet leads - is a three step process:

1. Add the proper disclosures to your web forms and obtain unambiguous consumer consent.

2. Capture and store a TrustedForm Certificate for each of your leads.

3. Verify in real-time that the proper disclosures were on your forms using the TrustedForm page scanning feature prior to calling.

Protect yourself from the risk of TCPA-driven lawsuits with TrustedForm from ActiveProspect. Call us today at 512-298-0978 or reach us at sales@activeprospect.com. We look forward to keeping your leads safe and profitable.