



Consent Re-Verification Using Telified-CR

Recent Court Cases Demonstrate How Operating With The Assumption Of Consent May Not Protect Companies From Violating The TCPA.

This document contains general guidelines and information collected from different sources. While we have given our best effort to provide clear and correct guidelines by interpreting US Telephone Consumer Protection Act (TCPA) regulations, PacificEast Research and IDICIA take no responsibility for any legal dispute arising in spite of or because of using these guidelines. Complying with the TCPA is the sole responsibility of entities making outbound communications to telephones. Please consult your legal advisor if you have any doubts on whether you need to comply with TCPA.

Trying to abide by the complex consumer consent requirements within the Telephone Consumer Protection Act, or TCPA, is difficult but as both the US Federal Trade and Communication Commissions step up their enforcement efforts, non-compliance with the TCPA can be very expensive **even if you believe you are complying**. Recent court cases have made it clear that intent to comply is not enough to avoid fines. This document is a summary of one such unintentional form of non-compliance that has recently triggered two court decisions against those communicating in ways they believed were completely reasonable and compliant. Additionally, we outline a possible solution for companies attempting to close this potentially expensive compliance gap.

The difficulty of compliance with the TCPA is both in its complexity and in its incompleteness. It is complex because it covers multiple categories of businesses: commercial companies, telemarketers, non-profits, political, etc. It is incomplete because while the TCPA may apply to all of these categories of businesses, only the rules for commercial telemarketing have been well documented. For non-commercial telemarketing uses like those of non-profits and businesses performing routine fraud-prevention or customer communications, the rules are not nearly as prescriptive leaving many details to be worked out in the courts. That “working out” process has started and banks and healthcare companies are getting a crash course in what “consumer consent” does **not** mean.

Two recent court decisions, *Soppet v. Enhanced Recovery Company, LLC*, 679 F.3d 637, 643 [7th Circuit, 2012] and *Breslow v. Wells Fargo Bank, N.A.*, 755 F.3d 1265 [11th Circuit, 2014], have held that companies are liable for un-consented calls or texts made to telephone numbers when those phone numbers have been recycled and reassigned to new consumers. In short, the defendants in both cases believed they had a consumer’s consent to communicate via a particular phone number. These companies had collected a consumer’s consent and were, as far as they were aware, operating in good faith and in compliance with the TCPA. However, in both cases the consumer had changed phone numbers and did not inform the company to whom they had granted consent. When that number was re-assigned to a new telephone subscriber, the company continued calling the consent number since they were not notified that the consent granting consumer’s information had changed. The assumption the defendants had made was that the consent was still valid for

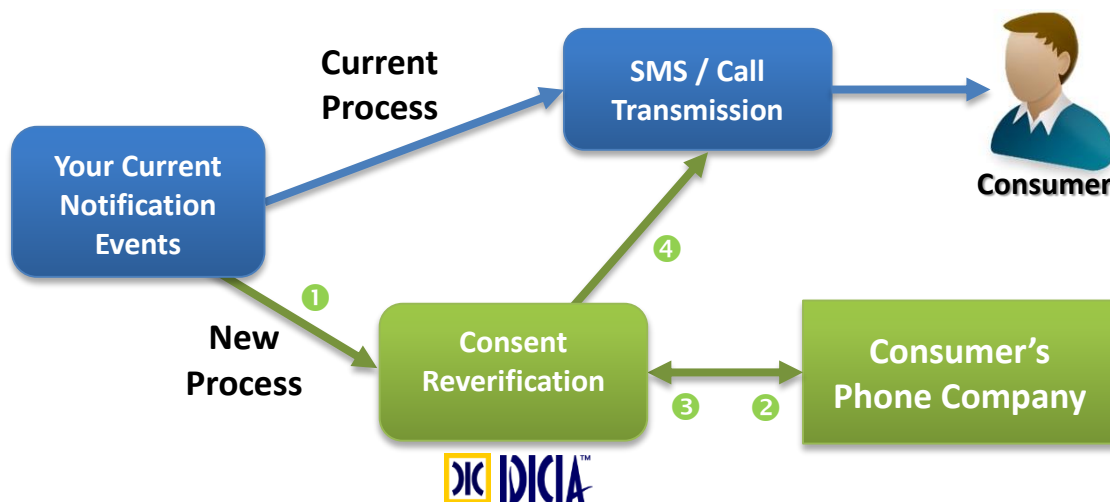
communication with a particular intended recipient. However, these two court decisions have clarified that the consent must come from the actual recipient of the communication, not from the “intended” recipient. In the Soppet case the court stated “consent to call a given number must come from its current subscriber.” With these decisions, companies find themselves in the position of not knowing if the consent they have is enough to remain compliant. The solution is to verify whether the consented phone number is still assigned to the original consenting party. In other words...

How can you confirm that you are calling the same person that gave you the consent?

This might sound like a very difficult question to answer, but fortunately it is not. To help companies establish if they still have consent they must verify that the consumer who granted consent is still in control of the consented phone number. To perform this task IDICIA has created a new configuration of their Telified™ brand called Telified CR that will provide what we are calling “consent re-verification”. Telified CR allows companies to very simply re-verify that the consenting consumer still owns the phone number in question. If so, then the consumer’s consent is still valid. However, if the number is disconnected or re-assigned, companies need to cease calling or texting that phone number.

How would my existing process change?

The Telified CR solution uses IDICIA’s existing platform for accessing telecom billing information systems to determine the appropriate phone company for each phone number, then verify with that phone company that the name and address they have on file matches the name and address of the consenting consumer. Consent can be re-verified either periodically or just prior to making any outbound communication.



IDICIA's Telified™ CR Solution can be integrated into virtually any automated SMS verification system. A company can perform consent re-verification immediately prior to each outbound communication or it can submit batch files for periodic re-verification.

Do we have any other options?

Given the recent court decisions, the ***only other choice*** left to companies to re-verify consent is to manually dial the numbers and verify that the number is still assigned to the person from whom they had received consent. However, it is not clear if that manual re-verification would be considered compliant. Even if the courts find manual verification acceptable, repeatedly calling customers is costly, time-consuming, annoying to the consumer and even a little suspicious for subscribers to have someone continually calling them to verify their name and address. While Telified CR does not yet have access to all phone records in the US, IDICIA estimates that over half of all US phone accounts can be verified using Telified CR. Customers of Telified CR are only charged for numbers that can be verified.

How can I tell if this will work for my company?

The next step is simple. Send us a confidential note to info@idicia.com and we can initiate a quick, simple and free test. You only need to send us a sample of the customers you wish to verify. The results you receive from IDICIA's Telified™ CR Solution will be placed into one of three categories:

1. Numbers which are assigned to the consenting party and can be contacted
2. Numbers which are no longer assigned to the consenting party or are disconnected
3. Numbers which cannot be confirmed and are therefore risky to contact.

All tests are processed within one of our high-security data centers. From this evaluation we can help you calculate the cost savings of utilizing IDICIA's Telified CR Solution to pre-screen your outbound communications.

Know who you are reaching on every call.

IDICIA wants to see you succeed. Let us provide you with the tools to protect your business.

###