

*October 12, 2021*

## **Buchalter TCPA Digest: The FCC Reassigned Number Database Is About to Go Live. Are You Ready?**

**By:** [Artin Betpera](#)

Calls to reassigned numbers have presented an endless source of legal risk for any company that calls or texts consumers for informational or marketing purposes. Reassigned number class actions brought under the Telephone Consumer Protection Act have resulted in eight-figure settlements, and present unique challenges when defending. For more than 10 years, the combination of murky regulations, and imperfect technological tools, have created a compliance minefield for callers.

Now, nearly three years after being announced, the FCC is about to take its long-awaited Reassigned Number Database (“RND”) live on November 1, 2021. The RND, together with the safe harbor attached to its use, shows promise as an effective tool to meaningfully reduce legal risk arising from calls to reassigned numbers.

This digest guide provides with an overview of the RND, orienting readers first with a brief background of the reassigned number conundrum. Readers will then be provided with an overview of the key aspects of the RND—both technical and legal—followed by a discussion of the practical issues presented by the new RND tools and rules. The goal of this guide will be to help prepare callers to develop new policies and protocols to integrate use of the RND, and understand how this new database fits within the big picture of TCPA compliance.

### **Why Have Calls to Reassigned Numbers Been Such a Problem?**

According to the FCC, there are approximately 35 million cell numbers that are disconnected and made available for reassignment each year. This churn rate of cell numbers raises the odds that a caller will unknowingly make a call to a reassigned cell phone number, and in doing so commit an inadvertent violation of the TCPA.

Calls to reassigned numbers carry a high risk of TCPA liability primarily due to the language in the statute requiring the consent of the “called party” to make calls using an automatic telephone dialing system, or artificial or pre-recorded voice. The FCC, as well as several lower and intermediate courts across the country have interpreted “called party” to mean the current subscriber or regular user of the phone line. Practically speaking, these rules mean that callers effectively lose consent the moment a cell number is reassigned.

Moreover, prior to the RND, callers had limited options, such as private commercial databases, for mitigating risk associated with reassigned number calls. However, the FCC recognized those services to be imperfect tools. Nor was there any safe harbor from TCPA liability attached to their use. Of note, the FCC had previously created a one-call safe harbor in a 2015 ruling (allowing callers to make a single call to a reassigned number without liability), but this token safe-harbor was struck down the D.C. Circuit Court of Appeals in 2018 on the basis that the one-call limit was arbitrary.

This milieu of circumstances has created a compliance minefield through which callers have had to tiptoe around for several years, sparking numerous TCPA class actions, and leading to an aggregate of hundreds of millions of dollars paid by callers in settlement of reassigned number claims.

### **What Is the RND?**

To understand how the RND works, it is helpful to first understand the process by which a number is reassigned.

Generally speaking, telephone numbers in the United States are part of the North American Numbering Plan (NANP). The NANP is a basic numbering scheme (consisting of 10 digits, including an area code, followed by a seven-digit number) that permits telecommunications services within the U.S. and other adjacent countries. Available numbers within the NANP are assigned to a cell phone subscriber. When the subscriber switches or disconnects their number, the number becomes “permanently disconnected,” meaning that the number has been permanently relinquished by the subscriber. After a 45-day aging period, that “permanently disconnected,” number is allowed to be reassigned to a new cell phone subscriber.

Simply stated, the RND is an actively updated database of telephone numbers that have been “permanently disconnected.” Under the FCC’s rules, providers/carriers that obtain NANP numbers are required to report all permanently disconnected numbers to the RND administrator. Large and medium sized voice providers began reporting their permanently disconnected numbers on April 15, 2020. Remaining small voice providers are required to begin reporting their numbers no later than October 15, 2021.

The database contains two datasets: phone numbers, and disconnect dates. The FCC has reported that the RND contains records of approximately 100 million telephone numbers reported as permanently disconnected. The FCC is requiring providers to report data on permanently disconnected numbers on the 15th day of each month.

### **How Do RND Queries Work?**

Callers are able to interact with, and utilize the RND by submitting queries that will help determine whether a particular phone number has been reassigned.

Callers may query the RND database using two data points. First, the telephone number. Second, either the date the caller obtained consent, or the last date the caller was able to verify that the consumer was at that telephone number. Once those two data points have been submitted to the RND, the caller will receive one of three results:

- |          |   |
|----------|---|
| Yes:     | The number has been permanently disconnected.   |
| No:      | The telephone number has not been permanently disconnected since the date of consent or last contact.                                   |
| No Data: | There is insufficient data to determine if the telephone number was permanently disconnected since the date of consent or last contact. |

From a practical standpoint, callers may assume that any number queried which returns a “yes” result has been reassigned, and is no longer associated with the intended recipient of the call. Thus, the number should not be called. Conversely, a “no” number means that the telephone number is still likely associated with the intended recipient of the call. Thus, the number may be called. No data results are inconclusive. As discussed below, this result presents a compliance dilemma for callers, the response to which is largely a question of risk tolerance.

From a technical standpoint, callers may perform queries in batch using a Web GUI (graphical user interface), SFTP (secure file transfer protocol), or API (application program interface). The RND’s web GUI is capable of processing batches of 50 queries at once, while larger batches (up to 250,000 queries at once) may be run using an SFTP or API. The RND’s website contains technical user guides with further details.

### **What Is the RND Safe Harbor?**

From a legal standpoint, the safe harbor is where the rubber meets the road for callers. There are a few elements, but in a nutshell, the safe harbor protects callers from TCPA liability if they inadvertently call a reassigned number in reliance on an erroneous “no” response from an RND query. The safe harbor has the following four elements:

1. The caller must have possessed prior express consent to call the number before its reassignment.
2. The caller calls the number after its reassignment.
3. Prior to calling, the caller had scrubbed the number against the most recent information in the RND, and received a response of “no.”
4. The call to the reassigned number was a result of the database erroneously returning a response of “no.”

In thinking through these elements, there are a few important things to note. First, to take advantage of the safe harbor, the caller must be able to demonstrate that it had the prior subscriber’s consent to call. Thus, the safe harbor will not apply if the caller is unable to establish initial consent.

Second, is a question of timing. More specifically, how often must numbers be scrubbed against the RND to meet the requirements of the safe harbor? The safe harbor requires that the number called has been scrubbed against “the most recent information in the RND.” According to the FCC’s orders, providers are required to submit disconnect data on the 15th day of each month. Thus, the “most recent information in the RND,” would seem to be after the 15th day of each month. Practically speaking, this means callers should consider monthly scrubs for numbers that are called on a regular basis or, at minimum, implementing safeguards to ensure that the last scrub of the number occurred after the most recent mid-month data dump into the RND.

### **What Is the Cost of Using the RND?**

The RND offers subscription tiers in t-shirt sizes: Extra Small, Small, Medium, Large, Extra Large, and so on. Subscription sizes vary in length of time (one to six months), and the number of inquiries during that time period (1,000 up to 180,000,000). Prices for RND subscription plans range from \$10 for the smallest one-month plan, up to \$210,600 for a six-month “jumbo” plan. The FCC has published a subscription pricing chart in their order [here](#).

### **How Does the RND Fit Within the Big Picture of TCPA Compliance?**

The RND will have more utility for some types of callers than others. Where call centers are making frequent or recurring calls to existing customers—such as in the context of debt servicing—the RND has the potential to be a very effective tool to mitigate TCPA risk arising out of wrong number calls. Logically, the risk that a number is reassigned increases the further out it is called from the date it was initially provided. Thus, the RND may not have as much utility to callers that engage in telemarketing, where numbers are usually called within a short time period after being provided to the caller (conversely, the RND may still have utility for aged leads).

Callers that utilize the RND will also need to make some judgment calls when it comes to risk. RND responses that come back with a “yes” or “no” are easy enough. Numbers that come back with a “yes” response should not be called, and numbers with a “no” response may be called with the benefit of the RND safe-harbor. However, callers will need to decide what to do with inconclusive “no data” responses. Calling “no data” numbers carries some legal risk given the uncertainty around the response, and because the call will be made outside of the RND safe-harbor. Obviously, the safest course is to not call “no data” numbers, but that sort of policy has the potential of hindering the caller’s ability to reach customers. Callers may also consider layering on other commercially available databases to further vet “no data” results. Ultimately, each caller will need to craft its own plan for dealing with “no data” results, considering its business objectives, the cost of compliance, and legal risk tolerances.

The RND also has its limits, specifically when it comes to *wrong* number calls. That is, numbers provided by consumers that are either inaccurate or false when provided. The RND’s data does not assist in confirming the association between the phone number called, and the intended recipient of the call, and its safe harbor does not apply in such situations. Accordingly, callers must

continue to rely on existing private commercial databases to help assess the correlation of the telephone number with the intended recipient of the call. As noted by the FCC in a recent order, such commercial databases “typically include a broader range of information to authenticate identities and other information about consumers that goes well beyond the narrow ability of this database to determine whether a number has been permanently disconnected since a date provided by the caller.”

Ultimately, the RND shows promise of substantially reducing the risk of reassigned number calls, particularly for industry sectors that make recurring calls to an existing customer base. It is certainly much more helpful than the FCC’s prior one-call token safe harbor. With the RND going live on November 1, 2021, now is an excellent time for callers to determine if and how they will incorporate this new tool into their compliance arsenal.

**[Artin Betpera](#)**

Shareholder

(949) 224-6422

[abetpera@buchalter.com](mailto:abetpera@buchalter.com)

This communication is not intended to create or constitute, nor does it create or constitute, an attorney-client or any other legal relationship. No statement in this communication constitutes legal advice nor should any communication herein be construed, relied upon, or interpreted as legal advice. This communication is for general information purposes only regarding recent legal developments of interest, and is not a substitute for legal counsel on any subject matter. No reader should act or refrain from acting on the basis of any information included herein without seeking appropriate legal advice on the particular facts and circumstances affecting that reader. For more information, visit [www.buchalter.com](http://www.buchalter.com).