Portfolio Media. Inc. | 111 West 19th Street, 5th floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Evaluating The Efficacy Of FCC's New Foreign Robocall Rules

By **Robert Gastner and Horace Payne** (August 6, 2019, 4:48 PM EDT)


Robert Gastner

On Aug. 1, 2019, the Federal Communications Commission approved new regulations intended to combat "spoofing" calls made by international actors. Through the passage of these new rules, the FCC is implementing a law passed by Congress last year, granting them the ability to regulate the transmission of calls that have been "spoofed" internationally.

In the past, FCC Chairman Ajit Pai noted the prevalence of such calls, saying, "scammers often robocall us from overseas, and when they do, they typically spoof their numbers to try and trick consumers." He continued by emphasizing the important role that the rules could play, saying, "We must attack this problem with every tool we have. With these new rules, we'll close the loopholes that hamstring law enforcement when they try to pursue international scammers and scammers using text messaging."

Increased scrutiny of international scammers flared with the arrival of the so-called "one ring" scam, which the FCC first addressed in May. Typically with this scam, unsuspecting victims receive a series of calls late at night from an unknown number which hang up after only one ring. Upon returning the call, victims are charged by the minute, like a 900 number. The scam works because callers use a number with a country code of Mauritania or Sierra Leone, 222 and 232, respectively, which resemble domestic area codes.

Another common tool for conducting scams is "spoofing," where a scammer can disguise his number as one with the same area code as the intended recipient. This recipient is more likely to answer the phone than for a totally random number, possibly assuming that it is a local business or another legitimate phone call. In this way, con artists are better able to gain access to victims. In 2018 alone, the FCC received more than 52,000 complaints about this practice; this helped to push impostor scams, where bad actors impersonating government, tech support or other such entities, to top the list of FCC complaints, with over half a million scams that led to a $488 million consumer loss and a median loss of $500 reported.

The Truth in Caller ID Act of 2009 had previously prohibited anyone located in the United States from engaging in spoofing with the intent to defraud, cause harm or wrongly obtain anything of value. However, the FCC was granted new statutory authority to scrutinize international calls from the RAY BAUM'S Act, which was passed as part of an omnibus spending bill last year. Prior to this legislation, the FCC did not have the ability to hold international scammers or scams conducted over text message into account.

Specifically, this legislation expanded the federal prohibition against knowingly transmitting misleading or inaccurate caller identification information to apply to: (1) persons outside the United States if the recipient is within the United States; and (2) text messages. The existing statutory caller identification requirements that applied to calls made using a telecommunications service or IP-enabled voice service (e.g., VoIP) were also expanded to apply to: (1) services interconnected with the public switched telephone network and that furnish voice communications using resources from the North American Numbering Plan; and (2) transmissions from a telephone facsimile machine, computer or other device to a telephone facsimile machine.

Violations of the federal government's fraudulent spoofing prohibitions face a potential civil forfeiture of up to $10,000 for each violation, or three times that amount for every day of a continuing violation, with a cap of $1 million for any continuing violation of any single act. Similarly, a criminal fine will be up to $10,000 for each violation, or three times that amount for every day of a continuing violation, and up to one year in prison.

Interestingly, robocalls have been historically regulated through the prohibitions of the Telephone Consumer Protection Act rather than more limited restrictions regarding number spoofing. However, the TCPA has faced criticism resulting from its strict liability fine regime. In 2018, more than 3,800 TCPA claims were filed in the federal system alone, not including those that settled before filing. In fact, a variable cottage industry has emerged, led by "professional plaintiffs" who make a business out of filing such claims.

Despite the ever-increasing volume of TCPA litigation, Americans still receive an incredibly high volume of robocalls, more than 47.8 billion in 2018 alone, according to YouMail. This represents an increase of more than 55% over the previous year. The problem being that TCPA lawsuits are disproportionately brought against American businesses because of the difficulty in collecting a civil judgment acquired in an American court against an entity located overseas. As a result, legitimate businesses based in the United States are targeted domestically by TCPA plaintiffs while internationally based scammers go unhindered. The result is that the explosion of private TCPA litigation in the United States has done little or nothing to actually prevent Americans from receiving unwanted robocalls.

However, there is some evidence to indicate that the federal government will be more effective at targeting bad actors overseas. In 2018, for example, the U.S. Securities and Exchange Commission used the Foreign Corrupt Practices Act to sue Credit Suisse Group AG, resulting in the Swiss-based firm agreeing to pay $30 million in fines to the SEC and $47 million in penalties. Additionally, judgments rendered in the United States can sometimes be enforced by seizing assets held domestically to recoup what is owed by the overseas debtor.

It is unlikely, however, that the international robocallers at issue have substantial ties to the United States, and the processes to enforce U.S. judgment overseas varies dramatically country by country. Due to the difficulty involved in the identification, prosecution and collection of penalties from the typical robocall scammer located overseas, it remains to be seen whether this expansion of the FCC's authority will deter international scammers' behavior. Moreover, the FCC's new international enforcement efforts will also probably have no effect on the suits being brought against legitimate American businesses for mistaken calls.

Regardless of the efficacy of the FCC's new rules, they are only part of the agency's multipronged approach to addressing the issue. The FCC has also recently adopted rules enabling voice service providers to block certain calls. It has encouraged the telecommunications industry to implement a framework called SHAKEN/STIR that is intended to verify caller ID information by "authenticating" the identity of the calling party to aid in preventing illegal spoofed calls, and the agency has proposed to mandate implementation of the SHAKEN/STIR framework should major voice service providers fail to implement it in a timely fashion. The agency hopes that these combined efforts will finally turn the tide in its battle against the seemingly ever-increasing flood of robocalls.

Robert J. Gastner is a member and Horace P. Payne III is a summer intern at Eckert Seamans Cherin & Mellott LLC.