

August 12, 2019

Federal Communications Commission: Progress Protecting Consumers from Illegal Robocalls

Robocalls are the top complaint received by the Federal Communications Commission (FCC) and a consistent congressional concern. In 2016, the FCC received 150,000 robocall-related complaints; in 2018, it received 232,000.

A robocall, also known as “voice broadcasting,” is any telephone call that delivers a pre-recorded message using an automatic (computerized) telephone dialing system, more commonly referred to as an automatic dialer or “autodialer.” Robocalls are popular with many industry groups, such as real estate, telemarketing, and direct sales companies. The majority of companies who use robocalling are legitimate businesses, but some are not. And those illegitimate businesses may not just be annoying consumers—they may also be trying to defraud them.

Despite the fact that most robocalls being made are illegal, the number of robocalls continues to grow in the United States. In 2016, the YouMail Robocall Index reported that an average of 2.4 billion robocalls were made per month. By July 2019, that figure was 4.7 billion. The all-time high was 5.2 billion in March 2019. (These figures include both legal and illegal robocalls.)

The FCC and the telecommunications industry have both taken steps to counter illegal robocalls. The telecommunications industry has developed new technologies and other tools to detect and block illegal robocalls. The FCC has taken steps to create a policy environment in which those tools can be implemented. The FCC has also expanded the scope of some existing rules and continues to target and fine illegal robocallers. The following provides a brief overview of the steps taken.

Call Blocking Initiatives

In November 2017, the FCC authorized telecommunications providers to block calls originating from numbers that should not originate calls, or that are invalid, unallocated, or unused, without violating call completion rules. The telecommunications industry has now widely implemented the blocking of numbers that should not originate calls, and numerous voice providers have implemented blocking of invalid, unallocated, and unused numbers. In December 2018, the FCC adopted a declaratory ruling clarifying that wireless providers are authorized to take measures to stop unwanted text messaging as well as unwanted calls. The FCC has also encouraged companies that block calls to establish an appeals process for erroneously blocked callers.

Caller ID Authentication

Illegitimate robocallers nearly always spoof their originating number. That is, they deliberately falsify the

Caller ID information they are transmitting to disguise their identity. One way to help consumers recognize spoofing and identify scams is to verify who is calling through Caller ID authentication. The telecommunications industry has been working on a framework of protocols, called Signature-based Handling of Asserted information using toKENs (SHAKEN) and Secure Telephony Identity Revisited (STIR), to ensure the accuracy of the Caller ID information. Once fully implemented, SHAKEN/STIR is expected to reduce the effectiveness of illegal spoofing and enable the identification of illegal robocallers. In November 2018 and February 2019, FCC Chairman Ajit Pai sent letters to telecommunications providers setting an end-of-2019 deadline for the industry to adopt the SHAKEN/STIR framework.

Call Traceback

Government authorities use the call traceback process to identify the origination of suspect telephone calls or text messages. Call traceback involves using the specific identifying characteristics of a call—date, time, Caller ID number, and dialed number—to track its routing from carrier to carrier. Caller ID spoofing makes it impossible to identify the caller’s billing name and address based on the Caller ID number. In November 2018, the FCC sent letters to voice providers asking them to assist industry efforts to trace scam robocalls that originate on or pass through their networks. Most providers affirmed their commitment to participate, and five providers that had been uncooperative have since taken steps to participate going forward.

Reassigned Numbers Database

When a consumer cancels service with a voice provider, the provider may reassign the number to a new consumer. If callers are unaware of the reassignment, they can make unwanted calls to the new consumer, unintentionally violating the Telephone Consumer Protection Act.

In March 2018, the FCC proposed that one or more databases be created to provide callers with the comprehensive and timely information they need to discover potential number reassignments before making a call. In December 2018, the Commission authorized the creation of a reassigned numbers database to enable callers to verify whether a telephone number has been permanently disconnected, and is therefore eligible for reassignment, before calling that number, thereby helping to protect consumers with reassigned numbers from receiving unwanted calls.

FCC Declaratory Ruling, June 2019

On June 6, 2019, the FCC adopted a declaratory ruling, “Advanced Methods to Target and Eliminate Unlawful

Robocalls.” The ruling empowers phone companies to block suspected illegal robocalls by default (allowing customers to opt-out) and asserts the FCC’s view that carriers can allow consumers to opt-in to more aggressive blocking tools (white-listing). (For additional information on this topic, see CRS Legal Sidebar LSB10333, *Robocall Regulation and Judicial Review*.) Both these tools seek to stop unwanted calls on the voice provider’s network before the calls reach the consumer’s phone.

Call-Blocking Programs

Call-blocking programs have become more popular and effective in the past few years. There are numerous blocking tools for different platforms, and the number of available tools is growing. Many service providers only offer these programs on an opt-in basis, limiting their potential impact. Providing a call-blocking program as the default option can significantly increase consumer participation while maintaining consumer choice.

White-List Programs

White-list programs require consumers to specify the telephone numbers from which they wish to receive calls—all other calls are blocked. Smartphones have provided a new way to implement white-list programs, because they store the consumer’s contact list. When the consumer’s contacts change, the white list can be updated. The declaratory ruling asserts the FCC’s view that nothing in the Communications Act of 1934 or the FCC’s rules prohibits a service provider from offering opt-in white-list programs.

FCC FNPRM, June 2019

Also on June 6, 2019, in conjunction with the declaratory ruling, the FCC adopted a third further notice of proposed rulemaking (FNPRM) on this topic. The FNPRM requested feedback on several proposals: a safe harbor for providers that implement blocking of calls that fail caller authentication under SHAKEN/STIR, protections for critical calls, mandating Caller ID authentication, and measuring the effectiveness of robocall solutions.

Safe Harbor for Call-Blocking Programs Based on Potentially Spoofed Calls

To ensure the effectiveness and integrity of the SHAKEN/STIR authentication framework, the FCC requested comment on proposed rules to allow voice providers, in certain instances, to block calls based on Caller ID authentication.

Protections for Critical Calls

The FCC requested comments on whether it should require voice providers offering call-blocking to maintain a “critical calls list” of emergency numbers that must not be blocked. Such lists would include, for example, the outbound numbers of 911 call centers and other government emergency outbound numbers. The blocking prohibition would apply only to SHAKEN/STIR-authenticated calls.

Mandating Caller ID Authentication

The FCC requested comments on its proposal to mandate implementation of the SHAKEN/STIR authentication

framework, if major voice providers fail to meet the end-of-2019 deadline for voluntary implementation.

Measuring the Effectiveness of Robocall Solutions

The FCC requested feedback on whether it should create a mechanism to provide information to consumers about the effectiveness of voice providers’ robocall solutions and, if so, how it should define and evaluate that effectiveness. The FCC also asked how it could obtain the information needed for such an evaluation.

Other FCC Actions Related to Robocalls

Other FCC actions to fight illegal robocallers include studies, continued enforcement actions, and implementation of additional anti-spoofing rules.

Reports on Deployment and Implementation of Call Blocking and Caller ID Authentication

The FCC has initiated two internal reports on the deployment status of technology solutions to eliminate robocalls, including the impact of call blocking on 911 and public safety. The reports are planned to be finished in June 2020 and a follow up report in June 2021.

The reports are to address the status of the availability to consumers of call blocking tools; any fees charged for the tools; the proportion of subscribers whose providers enable call blocking tools; the effectiveness of call blocking tools; and an assessment of the number of subscribers using call blocking tools. The reports are to assess the impact of FCC rule changes to allow providers to block calls from phone numbers on a Do-Not-Originate list and those that are from invalid, unallocated, or unused numbers. Further, the reports are to include status information on the implementation of the SHAKEN/STIR framework.

Continued Enforcement Actions

Since January 2017, the FCC has imposed or proposed about \$240 million in forfeitures against robocallers. One case involved an individual who made more than 96 million illegal robocalls over three months. Another involved an individual who conducted a large-scale robocalling campaign that marketed health insurance to vulnerable populations. In both cases, the illegal calls also disrupted an emergency medical paging service.

Extension of Robocall Ban to International Callers

In 2018, Congress amended the Communications Act of 1934 to include spoofing activities directed at U.S. consumers from callers outside the United States and caller ID spoofing using alternative voice and text messaging services. To implement these amendments, the FCC issued rules in July 2019 that expand and clarify the act’s prohibition on the use of misleading and inaccurate caller ID information.

Patricia Moloney Figliola, Specialist in Internet and Telecommunications Policy

Disclaimer

This document was prepared by the Congressional Research Service (CRS). CRS serves as nonpartisan shared staff to congressional committees and Members of Congress. It operates solely at the behest of and under the direction of Congress. Information in a CRS Report should not be relied upon for purposes other than public understanding of information that has been provided by CRS to Members of Congress in connection with CRS's institutional role. CRS Reports, as a work of the United States Government, are not subject to copyright protection in the United States. Any CRS Report may be reproduced and distributed in its entirety without permission from CRS. However, as a CRS Report may include copyrighted images or material from a third party, you may need to obtain the permission of the copyright holder if you wish to copy or otherwise use copyrighted material.