Congressional Research Service
Informing the legislative debate since 1914

Federal Communications Commission: Progress Protecting Consumers from Illegal Robocalls

April 10, 2020

Congressional Research Service
https://crsreports.congress.gov
R46311

CRS REPORT
Prepared for Members and
Committees of Congress

Congressional Research Service
Informing the legislative debate since 1914

SUMMARY

R46311

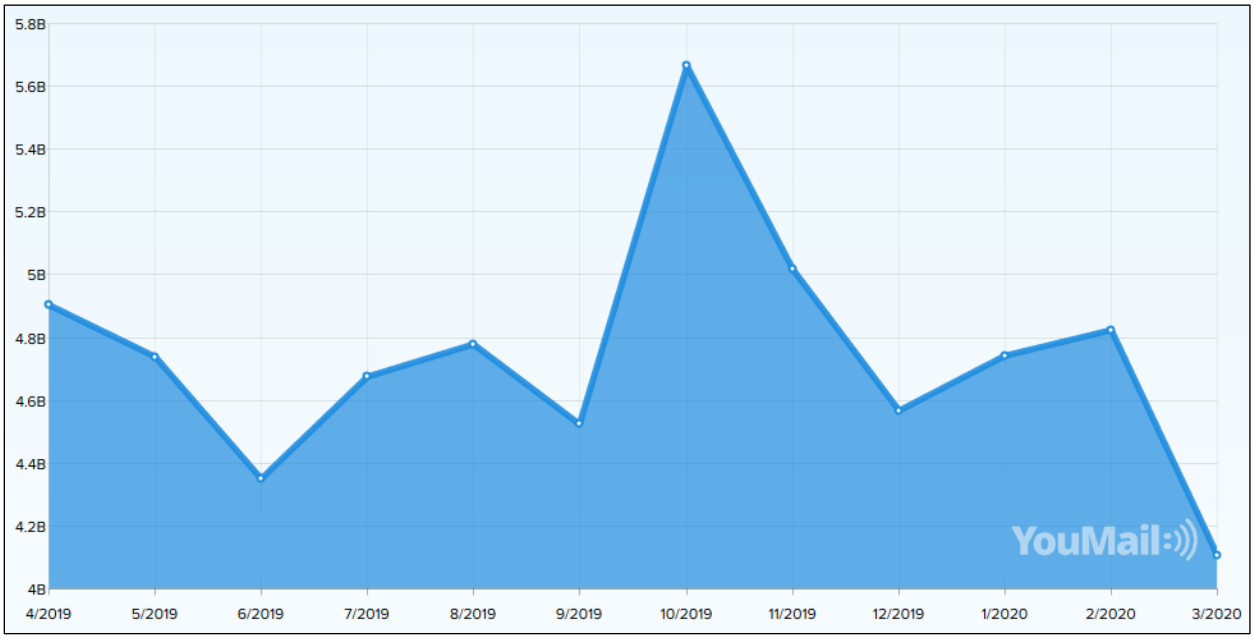
April 10, 2020

Patricia Moloney Figliola
Specialist in Internet and Telecommunications Policy

Federal Communications Commission: Progress Protecting Consumers from Illegal Robocalls

The number of robocalls continues to grow in the United States, and the figures tend to fluctuate based on the introduction of new government and industry attempts to stop them and robocallers' changing tactics to thwart those attempts (see **Figure**). In 2019, U.S. consumers received 58.5 billion robocalls, an increase of 22% from the 47.8 billion received in 2018, according to the YouMail Robocall Index. In 2016, the full first year the Robocall Index was tabulated, that figure was 29.1 billion calls—half the number of calls in 2019. Further, the Federal Communications Commission (FCC) states that robocalls make up its biggest consumer complaint category, with over 200,000 complaints each year—around 60% of all the complaints it receives. A robocall is any telephone call that delivers a pre-recorded message using an automatic (computerized) telephone dialing system. The Telephone Consumer Protection Act of 1991 (P.L. 102-243) regulates robocalls. Legal robocalls are used by legitimate call originators for political, public service, and emergency messages. Illegal robocalls are usually associated with fraudulent telemarketing campaigns. The FCC estimates that eliminating illegal scam robocalls would provide a public benefit of $3 billion annually. A survey by Truecaller, a company that tracks and blocks robocalls, puts that figure as high as $10.5 billion.

Figure. Robocalls per Month, April 2019 through March 2020
(in billions)



Source: Robocall Index, https://www.robocallindex.com.

Over the past three years, the FCC has pursued a multi-part strategy for combatting illegal robocalls. The agency has

- issued hundreds of millions of dollars in fines for violations of its Truth in Caller ID rules;
- expanded its rules to reach foreign calls and text messages;
- enabled voice service providers to block certain clearly unlawful calls before they reach consumers' phones;
- clarified that voice service providers may offer call-blocking services by default; and
- called on the industry to "trace back" illegal spoofed calls and text messages to their original sources.

Other wide-ranging steps by the FCC to stop illegal robocalls include mandating the implementation of call authentication technologies by the telecommunications industry, creating databases of numbers that should not be called, and establishing a reassigned numbers database. Major recent FCC regulatory actions include a June 2019 FCC Declaratory Ruling and Third Further Notice of Proposed Rulemaking, and a March 2020 FCC Order and Further Notice of Proposed Rulemaking. The FCC was empowered to take many of these actions by the Pallone-Thune Telephone Robocall Abuse Criminal Enforcement and Deterrence Act (TRACED Act) signed into law on December 30, 2019 (P.L. 116-105).

Although these steps appear to be having some impact, scammers remain determined to continue their attempts to defraud consumers using robocalls. Historically, decreases in the number of robocalls are sometimes followed shortly thereafter by spikes in those numbers, illustrating how robocallers continue to overcome measures to stop them (e.g., by changing their originating numbers). Most of the tools being used against robocalls have been developed recently, while some are still under development. Therefore, it may take telecommunications providers some time to fully implement them, and it may be some time before a long-term and ongoing decrease in robocall numbers will be realized. The positive impacts of FCC initiatives on fraudulent robocalls, as well as potential negative impacts on the telemarketing industry due to blocking legitimate calls, may be the subject of continued oversight by Congress.

Contents

Introduction 1
The Telephone Robocall Abuse Criminal Enforcement and Deterrence Act 3
Ongoing Efforts to Combat Robocalls 3
Call Blocking Initiatives 3
Do Not Originate Registry and Other Call Blocking 4
2020 FCC Report on Call Blocking 4
Caller ID Authentication 4
Call Traceback 5
Reassigned Numbers Database 5
FCC Declaratory Ruling and Third Further Notice of Proposed Rulemaking, June 2019 5
Declaratory Ruling 6
Call-Blocking Programs (Opt Out) 6
White-List Programs (Opt In) 6
Third Further Notice of Proposed Rulemaking 6
Safe Harbor for Call-Blocking Programs Based on Potentially Spoofed Calls 6
Protections for Critical Calls 7
Mandating Caller ID Authentication 7
Measuring the Effectiveness of Robocall Solutions 7
FCC Order and Further Notice of Proposed Rulemaking, March 2020 7
Order 7
Further Notice of Proposed Rulemaking 8
Other FCC Actions Related to Robocalls 8
Ongoing Enforcement Actions 8
Extension of Robocall Ban to International Callers 8
Hospital Robocall Protection Group 9
Outlook 9

Figures

Figure 1. Robocalls per Month, April 2019 through March 2020 2

Contacts

Author Information 9

Introduction

Robocalls are the top complaint received by the Federal Communications Commission (FCC) and a consistent congressional concern. 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."

The Telephone Consumer Protection Act of 1991 (TCPA)[1] regulates robocalls. Legal robocalls are used by legitimate call originators for political, public service, and emergency messages, which are legal. Other legitimate uses can be, for example, to announce school closures or to remind consumers of medical appointments. Illegal robocalls are usually associated with fraudulent telemarketing campaigns, but an illegal robocall under the TCPA does not necessarily mean that the robocall is fraudulent.[2] Illegal, fraudulent calls usually include misleading or inaccurate Caller ID information to disguise the identity of the calling party and trick called parties, which is called "spoofing." Scammers sometimes use "neighbor spoofing" so it will appear that an incoming call is coming from a local number. They may also spoof a number from a legitimate company or a government agency that consumers know and trust.[3] Like robocalls more generally, spoofing can also be used for legitimate purposes, such as to hide the number of a domestic violence shelter or an individual employee extension at a business or government agency. This report addresses robocalls that are both illegal under the TCPA as well as intended to defraud, not robocalls that are defined only as illegal.

The number of robocalls continues to grow in the United States, and the figures tend to fluctuate based on the introduction of new government and industry attempts to stop them and robocallers' changing tactics to thwart those attempts (see **Figure 1**). In 2019, U.S. consumers received 58.5 billion robocalls, an increase of 22% from the 47.8 billion received in 2018, according to the YouMail Robocall Index.[4] In 2016, the full first year the Robocall Index was tabulated, that figure was 29.1 billion calls—half the number of calls in 2019.[5] Further, the FCC states that robocalls make up its biggest consumer complaint category, with over 200,000 complaints each year—around 60% of all the complaints it receives.

Over the past three years, the FCC has pursued a multi-part strategy for combatting spoofed robocalls. The agency has

- issued hundreds of millions of dollars in fines for violations of its Truth in Caller ID rules;[6]

[1] P.L. 102-243, 47 U.S.C. §227. The TCPA governs other aspects of telemarketing outside the scope of this report.

[2] For example, it is illegal to make a marketing robocall to a cellphone without written consent. That call would not necessarily be intended to defraud the consumer. The TCPA also treats calls to mobile phones differently than calls to landlines and treats calls to consumers differently than calls to businesses. For additional information about how the TCPA regulates robocalls, see CRS Report R45070, *Protecting Consumers and Businesses from Fraudulent Robocalls*, by Patricia Moloney Figliola.

[3] Federal Communications Commission, Consumer Guide, "Caller ID Spoofing," January 6, 2020, https://www.fcc.gov/consumers/guides/spoofing-and-caller-id.

[4] Mike Snider, "Robocalls Rang Up a New High in 2019: Two or More Daily Is Average in Some States," *USA Today*, January 15, 2020 (updated January 17, 2020), https://www.usatoday.com/story/tech/2020/01/15/robocalls-americans-got-58-5-billion-2019/4476018002/.

[5] YouMail Robocall Index, Historical Robocalls By Time, https://robocallindex.com/history/time. The Robocall Index includes both legal and illegal robocalls.

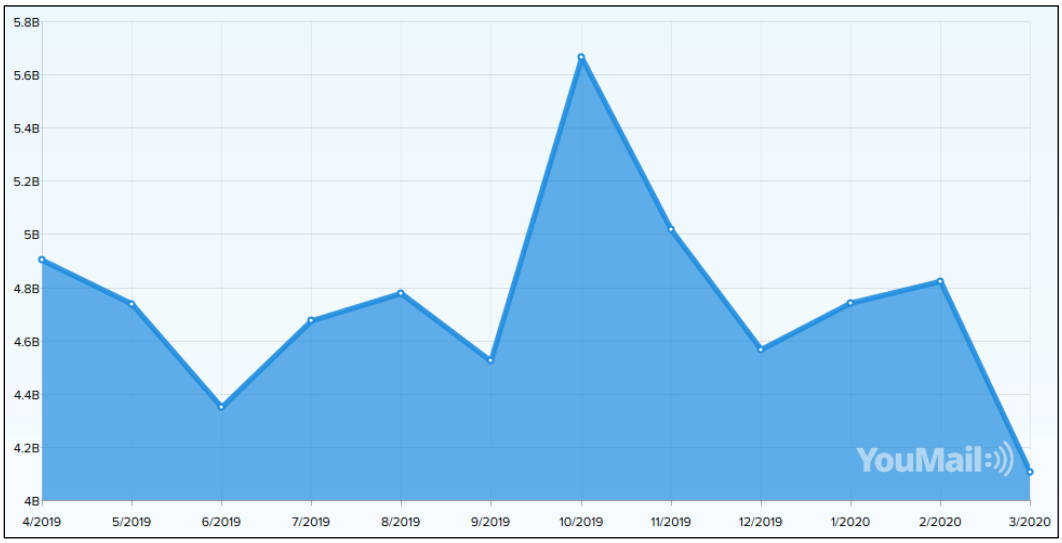
[6] Under the Truth in Caller ID Act, FCC rules prohibit anyone from transmitting misleading or inaccurate caller ID information with the intent to defraud, cause harm or wrongly obtain anything of value. Anyone who is illegally

- expanded its rules to reach foreign calls and text messages;
- enabled voice service providers to block certain clearly unlawful calls before they reach consumers' phones;
- clarified that voice service providers may offer call-blocking services by default; and
- called on the industry to "trace back" illegal spoofed calls and text messages to their original sources.

The FCC estimates that eliminating illegal scam robocalls would provide a public benefit of $3 billion annually.[7] A survey by Truecaller, a company that tracks and blocks robocalls, puts that figure as high as $10.5 billion.[8]

Figure 1. Robocalls per Month, April 2019 through March 2020

(in billions)



Source: Robocall Index, https://www.robocallindex.com.

spoofing can face penalties of up to $10,000 for each violation. However, spoofing is not always illegal. There are legitimate, legal uses for spoofing, such as when a doctor calls a patient from her personal mobile phone and displays the office number rather than the personal phone number or a business displays its toll-free call-back number.

[7] Federal Communications Commission, Declaratory Ruling and Third Further Notice of Proposed Rulemaking, "In the Matter of Advanced Methods to Target and Eliminate Unlawful Robocalls (CG Docket 17-59) and Call Authentication Trust Anchor (WC Docket No. 17-97)," FCC 19-51, June 6, 2019, https://docs.fcc.gov/public/attachments/FCC-19-51A1.pdf. (Hereinafter, "Declaratory Ruling and Third Further Notice of Proposed Rulemaking.")

[8] A 2019 survey estimated that spoofing fraud affected one in six Americans and cost approximately $10.5 billion in a single 12-month period. Kim Fai Kok, *Truecaller Insights: Phone Scams Cause Americans to Lose $10.5 Billion in Last 12 Months Alone*, April 17, 2019, https://truecaller.blog/2019/04/17/truecaller-insights-2019-us-spamphone-scam-report. The FCC uses "the reasonable cost of an unwanted call is 10 cents" times the number of scam calls, while Truecaller uses "the average phone scam victim in the survey reported losing $244" times the total number of phone scam victims. The FCC may be measuring the inconvenience of receiving a call while Truecaller may be measuring money actual lost from a phone scam.

The Telephone Robocall Abuse Criminal Enforcement and Deterrence Act

The Pallone-Thune Telephone Robocall Abuse Criminal Enforcement and Deterrence Act (TRACED Act) empowered the FCC to take specific actions to fight illegal robocalls; it was signed into law on December 30, 2019 (P.L. 116-105). The law requires the FCC to

- administer a forfeiture penalty for violations (with or without intent) of the prohibition on certain robocalls;
- promulgate rules establishing when a provider may block a voice call based on information provided by the call authentication framework, called Secure Telephony Identity Revisited (STIR) and Signature-based Handling of Asserted information using toKENs (SHAKEN) (together known as "STIR/SHAKEN"), and establish a process to permit a calling party adversely affected by the framework to verify the authenticity of its calls;
- initiate a rulemaking to help protect subscribers from receiving unwanted calls or texts from a caller using an unauthenticated number;
- assemble, in conjunction with the Department of Justice, an interagency working group to study and report to Congress on the enforcement of the prohibition of certain robocalls; and
- initiate a proceeding to determine whether its policies regarding access to number resources could be modified to help reduce access to numbers by potential robocall violators.

STIR/SHAKEN is seen by many, including the FCC, as a particularly important part of achieving the projected cost savings associated with eliminating illegal robocalls. STIR/SHAKEN must be implemented by June 30, 2021.[9]

Ongoing Efforts to Combat Robocalls

Both the telecommunications industry and the FCC are taking 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.

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. 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.

[9] Federal Communications Commission, News Release, "FCC Mandates That Phone Companies Implement CallerID Authentication to Combat Spoofed Robocalls," March 30, 2020, https://docs.fcc.gov/public/attachments/DOC-363399A1.pdf.

Do Not Originate Registry and Other Call Blocking

The telecommunications industry has now widely implemented the blocking of numbers that should not originate calls, called the "Do Not Originate" (DNO) Registry. In November 2017, the FCC promulgated rules on the creation and use of the DNO Registry. The rules explicitly allow service providers to block calls from two categories of number: (1) numbers that the subscriber has asked to be blocked, such as "in-bound only" numbers (numbers that should not ever originate a call); and (2) unassigned numbers, as the use of such a number indicates that the calling party is intending to defraud a consumer.

USTelecom, a trade association representing telecommunications-related businesses in the United States, maintains this registry and works with industry to implement DNO call blocking for in-bound numbers associated with government agencies.

2020 FCC Report on Call Blocking

On December 20, 2019, the FCC released a public notice seeking comments for its first of two staff reports on call blocking issues mandated by the TRACED Act.[10] The agency asked for comments on

- the availability and effectiveness of call blocking tools offered to consumers;
- the impact of the FCC's actions on illegal calls;
- the impact of call blocking on 911 services and public safety; and
- any other issues parties would like to see addressed.

Comments were due January 29, 2020, and reply comments were due February 28, 2020.[11]

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. Over the past few years, the telecommunications industry developed a set of protocols, the STIR/SHAKEN framework that enables phone companies to verify that the Caller ID information transmitted with a call matches the caller's phone number. Once fully implemented, STIR/SHAKEN is expected to reduce the effectiveness of illegal spoofing and enable the identification of illegal robocallers. The FCC mandated the adoption of STIR/SHAKEN on March 31, 2020. These steps are discussed in detail in the section of this report, "FCC Order and Further Notice of Proposed Rulemaking, March 2020."

[10] Federal Communications Commission, Public Notice, "Consumer and Governmental Affairs Bureau Seeks Input for Report on Call Blocking," DA 19-1312, December 20, 2019. The notice was published in the *Federal Register* on December 30, 2019. The first staff report was published in February 2019 and is available at https://docs.fcc.gov/public/attachments/DOC-356196A1.pdf.

[11] Comments and reply comments are available on the FCC Electronic Filing System at https://www.fcc.gov/ecfs/search/filings?date_received=%5Bgte%5D2020-1-1%5Blte%5D2020-2-28&q=%22call%20blocking%22%20AND%20(proceedings.name:((17%5C-97)%20OR%20(17%5C-59))%20OR%20proceedings.description:((17%5C-97)%20OR%20(17%5C-59)))&sort=date_disseminated,DESC.

Call Traceback

More than 30 voice service providers participate in the USTelecom Industry Traceback Group (ITG), which was formally established in May 2016. The ITG is a collaborative effort of companies across the wireline, wireless, voice over internet protocol, and cable industries that actively trace and identify the source of illegal robocalls. The ITG coordinates with federal and state law enforcement agencies to identify non-cooperative providers so those agencies can take enforcement action, as appropriate.

During 2019, ITG members conducted more than 1,000 tracebacks, associated with more than 10 million illegal robocalls. This activity has resulted in more than 20 subpoenas and/or civil investigative demands from federal and state enforcement agencies.[12] The ITG published its first status report in January 2020.[13]

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. On January 24, 2020, the FCC requested public comment on the technical requirements developed for the database by the North American Numbering Council (NANC).[14] Comments were due February 24, 2020, and reply comments were due March 9, 2020.

FCC Declaratory Ruling and Third Further Notice of Proposed Rulemaking, June 2019

On June 6, 2019, the FCC adopted a declaratory ruling and third further notice of proposed rulemaking (FNPRM), "Advanced Methods to Target and Eliminate Unlawful Robocalls and Call Authentication Trust Anchor."[15]

---

[12] USTelecom, Industry Traceback Group 2019 Status Report, January 2020, https://www.ustelecom.org/wp-content/uploads/2020/01/USTelecom_ITG_2019_Progress_Report.pdf.

[13] The status report is available online at https://www.ustelecom.org/wp-content/uploads/2020/01/USTelecom_ITG_2019_Progress_Report.pdf. General information about the ITG is available at https://www.ustelecom.org/the-ustelecom-industry-traceback-group-itg/.

[14] Federal Communications Commission, Public Notice, "Wireline Competition Bureau and Consumer and Government Affairs Bureau Seek Comment on Technical Requirements for Reassigned Numbers Database," DA 20-105, January 24, 2020, https://docs.fcc.gov/public/attachments/DA-20-105A1.pdf. The NANC's recommended Technical Requirements Document for the Database is available at https://docs.fcc.gov/public/attachments/DOC-361954A1.pdf.

[15] Federal Communications Commission, Declaratory Ruling and Third Further Notice of Proposed Rulemaking, "Advanced Methods to Target and Eliminate Unlawful Robocalls," FCC-19-51, June 6, 2019,

Declaratory Ruling

The declaratory ruling empowers phone companies to block suspected illegal robocalls by default (customers may opt out) and asserts the FCC's view that carriers can allow consumers to opt in to more aggressive call-blocking tools, known as white-listing. Both blocking by default and opt-in white-listing tools seek to stop unwanted calls on the voice provider's network before calls reach the consumer's phone.[16]

Call-Blocking Programs (Opt Out)

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 (Opt In)

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.

Third Further Notice of Proposed Rulemaking

The FNPRM requested feedback on several proposals: a safe harbor for providers that implement blocking of calls that fail caller authentication under STIR/SHAKEN, protections for critical calls, mandating Caller ID authentication, and measuring the effectiveness of robocall solutions. Comments were due on July 24, 2019, and reply comments were due on August 23, 2019.[17]

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

The FCC proposed a narrow safe harbor for voice service providers that offer call-blocking programs that take into account (1) whether a call has been properly authenticated under the SHAKEN/STIR framework and (2) may potentially be spoofed. The safe harbor limits liability for voice service providers if they block a legal robocall. Among other elements, the FCC proposed a safe harbor for voice service providers that choose to block calls that fail SHAKEN/STIR authentication and asked whether there might be other instances where authentication would fail. The FCC also asked how it could ensure that wanted calls are not blocked and sought comment as to how to identify and remedy the blocking of wanted calls.

[16] For additional information on this topic, see CRS Legal Sidebar LSB10333, *Robocall Regulation and Judicial Review*, by Eric N. Holmes.

[17] Comments and reply comments are available online at https://www.fcc.gov/ecfs/search/filings?date_received=%5Bgte%5D2019-6-6%5Blte%5D2019-8-23&q=(proceedings.name:((17%5C-57*)%20OR%20(17%5C-97))%20OR%20proceedings.description:((17%5C-57*)%20OR%20(17%5C-97)))&sort=date_disseminated,DESC.

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 services. The blocking prohibition would apply only to STIR/SHAKEN-authenticated calls.

Mandating Caller ID Authentication

The FCC requested comments on its proposal to mandate implementation of the STIR/SHAKEN authentication framework, if major voice providers fail to meet the end-of-2019 deadline for voluntary implementation. This is the topic of the FCC order issued on March 31, 2020, and is discussed in detail in the next section of this report, "FCC Order and Further Notice of Proposed Rulemaking, March 2020."

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.

FCC Order and Further Notice of Proposed Rulemaking, March 2020

The FCC published its latest guidance and proposals on March 31, 2020, in a new order and FNPRM.[18]

Order

The new rules require implementation of Caller ID authentication using STIR/SHAKEN. Specifically, the rules require "all originating and terminating voice service providers to implement STIR/SHAKEN in the Internet Protocol (IP) portions of their networks by June 30, 2021, a deadline that is consistent with Congress's direction in the recently-enacted TRACED Act," described earlier in, "The Telephone Robocall Abuse Criminal Enforcement and Deterrence Act." Most experts say that widespread deployment of STIR/SHAKEN will reduce the effectiveness of illegal spoofing, allow law enforcement to identify bad actors more easily, and help phone companies to identify calls with illegally spoofed Caller ID information before those calls reach their subscribers.

[18] Federal Communications Commission, Report and Order and Further Notice of Proposed Rulemaking, "Call Authentication Trust Anchor (WC Docket 17-97) and Implementation of TRACED Act Section 6(a)—Knowledge of Customers by Entities with Access to Numbering Resources (WC Docket 20-67)," FCC 20-42, March 31, 2020, https://www.fcc.gov/document/mandating-stirshaken-combat-spoofed-robocalls-0. (Hereinafter, "Call Authentication Trust Anchor.")

Further Notice of Proposed Rulemaking

The FNPRM requests public comments on

- expanding the STIR/SHAKEN implementation mandate to cover intermediate voice service providers;
- extending the implementation deadline by one year for small voice service providers pursuant to the TRACED Act;
- adopting requirements to promote caller ID authentication on voice networks that do not rely on IP technology; and
- implementing other aspects of the TRACED Act.

Comments to the FNPRM are due on May 15, 2020, and reply comments are due on May 29, 2020.[19]

Other FCC Actions Related to Robocalls

Other FCC actions to fight illegal robocallers include ongoing enforcement actions, an extension of a robocall ban to international callers, and the establishment of a hospital robocall protection group.

Ongoing 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 the course of 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 disrupted an emergency medical paging service.[20]

Extension of Robocall Ban to International Callers

In 2018, Congress amended the Communications Act of 1934 to prohibit 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 expanded the act's prohibition on the use of misleading and inaccurate Caller ID information.[21]

[19] Federal Communications Commission, "Call Authentication Trust Anchor Implementation of TRACED Act Section 6(a)—Knowledge of Customers by Entities with Access to Numbering Resources, WC Docket 17-97 and WC Docket 20-67, March 31, 2020, https://docs.fcc.gov/public/attachments/FCC-20-42A1.pdf.

[20] See https://www.fcc.gov/about-fcc/fcc-initiatives/fccs-push-combat-robocalls-spoofing.

[21] Federal Communications Commission, Report and Order, "Implementing Section 503 of RAY BAUM'S Act," (FCC-19-73), August 1, 2020, https://www.fcc.gov/document/fcc-bans-malicious-spoofing-text-messages-foreign-robocalls-0.

Hospital Robocall Protection Group

The TRACED Act of 2019 required the FCC to establish a Hospital Robocall Protection Group. For most consumers, robocalls are a potentially fraudulent nuisance. For hospitals, though, the robocalls can present challenges that are increasingly threatening doctors and patients:

> At Tufts Medical Center, administrators registered more than 4,500 calls between about 9:30 and 11:30 a.m. on April 30, 2018, said Taylor Lehmann, the center's chief information security officer. Many of the messages seemed to be the same: Speaking in Mandarin, an unknown voice threatened deportation unless the person who picked up the phone provided their personal information.[22]

The FCC began soliciting nominations for the group in March 2020. Once established, the group is to be charged to develop and issue best practices regarding (1) how voice service providers can better combat unlawful robocalls made to hospitals; (2) how hospitals can better protect themselves from such calls; and (3) how the federal government and state governments can help combat such calls.[23]

Outlook

The FCC has taken wide-ranging steps to stop illegal robocalls, including imposing fines on law breakers; mandating the implementation of call authentication technologies by the telecommunications industry; creating databases of numbers that should not be called; and providing regulatory permission to implement call blocking. Although these steps appear to be having some impact, scammers remain determined to continue their attempts to defraud consumers using robocalls. Historically, decreases in the number of robocalls are sometimes followed shortly thereafter by spikes in those numbers, illustrating how robocallers continue to overcome measures to stop them (e.g., by changing their originating numbers). Most of the tools being used against robocalls have been developed recently, while some are still under development. Therefore, it may take telecommunications providers some time to fully implement them, and it may be some time before a long-term and ongoing decrease in robocall numbers will be realized. The positive impacts of FCC initiatives on fraudulent robocalls, as well as potential negative impacts on the telemarketing industry due to blocking legitimate calls, may be the subject of continued oversight by Congress.

Author Information

Patricia Moloney Figliola
Specialist in Internet and Telecommunications Policy

[22] Tony Romm, "Robocalls Are Overwhelming Hospitals and Patients, Threatening a New Kind of Health Crisis," *Washington Post*, June 17, 2019, https://www.washingtonpost.com/technology/2019/06/17/robocalls-are-overwhelming-hospitals-patients-threatening-new-kind-health-crisis/.

[23] Federal Communications Commission, News Release, "FCC Launches New Hospital Robocall Protection Group," March 25, 2020, https://www.fcc.gov/document/fcc-launches-new-hospital-robocall-protection-group.

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.