United States Government Accountability Office

Report to Congressional Committees

December 2019

FAKE CALLER ID SCHEMES Information on Federal Agencies' Efforts to Enforce Laws, Educate the Public, and Support

Accessible Version

GAO-20-153

December 2019

FAKE CALLER ID SCHEMES
Information on Federal Agencies' Efforts to Enforce Laws, Educate the Public, and Support Technical Initiatives

GAO Highlights

Highlights of GAO-20-153, a report to congressional committees

Why GAO Did This Study

Unwanted phone calls, which may also involve spoofing, consistently rank among the top consumer complaints to FCC and FTC. In recent years, consumers have lost millions of dollars—and been deceived into providing financial or other sensitive information or purchasing falsely advertised products—due to schemes using these calls. FCC, FTC, and DOJ have efforts aimed at combatting the fraudulent use of caller ID spoofing.

Recently enacted federal legislation included a statutory provision for GAO to review federal efforts to combat the fraudulent use of caller ID spoofing. This report examines (1) what is known about caller ID spoofing schemes, including any recent trends; (2) federal agency enforcement and consumer education efforts; and (3) the status of industry efforts to develop technologies to combat spoofing, and FCC's role in these efforts.

To address these objectives, GAO reviewed consumer complaint data from FCC and FTC from 2015 through 2018; reviewed investigation and enforcement information from FCC, FTC, and DOJ; and interviewed agency officials and representatives from 23 nonfederal stakeholders, including industry associations, voice service providers, call blocking and analytics services, mobile phone manufacturers, consumer groups, and a standards body. GAO also reviewed relevant agency documentation and assessed agency efforts against key practices for consumer education and interagency collaboration identified in GAO reports.

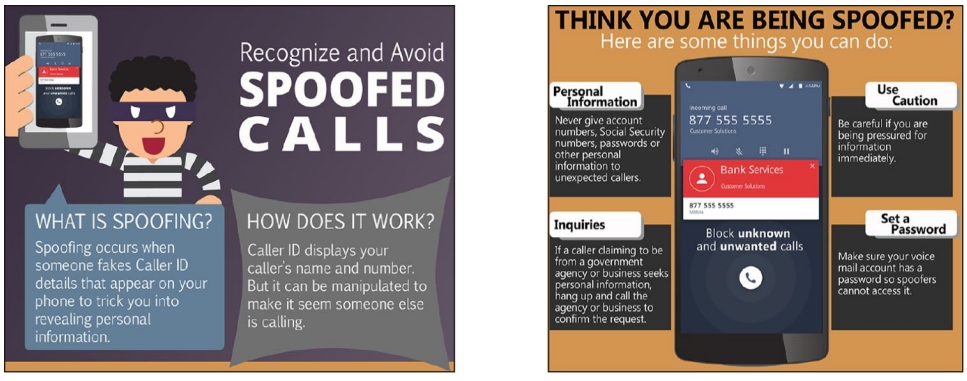
View GAO-20-153. For more information, contact Andrew Von Ah at (202) 512-2834 or VonahA@gao.gov.

What GAO Found

Transmitting fake caller ID information with a phone call, also referred to as "spoofing," is in many cases illegal—and is used in schemes to obtain money and personal information or generate telemarketing leads. Complaints submitted to the Federal Communications Commission (FCC) and the Federal Trade Commission (FTC), both of which work to protect consumers from spoofing, suggest that spoofing is a growing issue.

FCC, FTC, and the Department of Justice (DOJ) identified 62 enforcement cases they have brought since 2006 involving spoofing. Enforcement can be challenging, as it can be difficult to identify the source of spoofed calls, and scammers may be based overseas. Nevertheless, GAO found that the agencies prioritize their spoofing-related enforcement actions based in part on the level of harm perpetrated against the public and generally follow key practices identified by GAO for effective collaboration. Additionally, FCC and FTC have proposed changes to law to enhance the effectiveness of their enforcement efforts, such as a change that would allow FCC more time to bring certain enforcement actions. Furthermore, FCC's and FTC's consumer education efforts related to spoofing align with key practices for collaboration and consumer education. For example, FCC and FTC have developed consistent and clear messages related to spoofing.

FCC's Graphic on How to Avoid Being Victimized by Spoofing



Source: Federal Communications Commission (FCC). | GAO-20-153

Several major telecommunications carriers are taking key steps to put an industry-developed technical system in place designed to reduce spoofing by December 2019, which FCC has encouraged in line with federal guidance. This system is intended to enable carriers to verify whether a caller has a right to use the caller ID being transmitted with the call. Carriers can use this information to better determine whether to block or warn consumers about the incoming call. Stakeholders cautioned that the system cannot determine whether a caller has fraudulent intentions but only whether the caller is using a spoofed number. FCC has followed relevant federal guidance in participating in the development of this system by, for example, encouraging industry to accelerate deployment of the system, monitoring industry's progress, and providing input into the process.

Contents

Tables

Figures

Abbreviations

ATIS	Alliance for Telecommunications Industry Solutions
DNC Registry	National Do Not Call Registry
DOJ	Department of Justice
FCC	Federal Communications Commission
FTC	Federal Trade Commission
IP	Internet Protocol
IRS	Internal Revenue Service
SIP	Session Initiation Protocol
VoIP	Voice over Internet Protocol

U.S. GOVERNMENT ACCOUNTABILITY OFFICE
441 G St. N.W.
Washington, DC 20548

December 18, 2019

The Honorable Roger Wicker
Chairman
The Honorable Maria Cantwell
Ranking Member
Committee on Commerce, Science, and Transportation
United States Senate

The Honorable Frank Pallone Jr.
Chairman
The Honorable Greg Walden
Ranking Member
Committee on Energy and Commerce
House of Representatives

Robocalls and other unwanted phone calls consistently rank among the top consumer complaints to the Federal Communications Commission (FCC) and the Federal Trade Commission (FTC).[1] Many robocallers also transmit false caller ID information with these calls, which then shows up on a recipient's caller ID display—a practice often referred to as "spoofing." By spoofing a phone number—such as the number of a government agency or a reputable company—the caller is able to disguise their true identity and may also be able to immediately establish some level of credibility with the call recipient. In recent years, consumers have lost millions of dollars—and been deceived into providing financial or other sensitive information or purchasing falsely advertised products—due to such schemes.

[1]The FCC generally considers robocalls to consist of calls using a prerecorded or artificial voice, rather than calls made using an automatic telephone dialing system, telemarketing calls, or other violations of the Telephone Consumer Protection Act. This practice is in large part because consumers know when they receive a robocall but generally cannot tell whether a call was made using an automatic telephone dialing system.

Spoofing is illegal when done with the intent to defraud, cause harm, or wrongfully obtain anything of value.[2] In addition, with some exceptions, it is an abusive telemarketing practice and a violation of FTC regulations for telemarketers to spoof or block caller ID.[3] FCC regulates communications, and FTC protects consumers from unfair and deceptive business practices. In addition, the Department of Justice (DOJ) enforces federal consumer fraud statutes, among other laws, which may involve spoofing. All three agencies may take enforcement actions against those who use illegal spoofing in different kinds of schemes. In addition, in 2018, FCC, in coordination with FTC, was directed by statute to undertake efforts to educate consumers about caller ID spoofing.[4] FCC has also worked with the telecommunications industry on a system to enable telephone companies and other voice service providers to verify caller ID information.[5]

[2]The Communications Act of 1934, as amended by the Truth in Caller ID Act of 2009, prohibits any person from knowingly transmitting misleading or inaccurate caller identification information with the intent to defraud, cause harm, or wrongfully obtain anything of value, subject to certain exceptions. Communications Act of 1934, Pub. L. No. 73-416, 48 Stat. 1064 (1934), *as amended by* Pub. L. No. 111-331, 124 Stat. 3572 (2010), codified at 47 U.S.C. § 227(e)(1). The prohibition does not apply to (1) lawfully authorized investigative, protective, or intelligence activity of a law enforcement agency of the United States, a state, or a political subdivision of a state, or of an intelligence agency of the United States; or (2) activity engaged in pursuant to a court order that specifically authorizes the use of caller identification manipulation. 47 C.F.R. § 64.1604(b).

[3]16 C.F.R.§ 310.4(a)(8).There is an exception for substituting the name or the number of a seller or charitable organization on behalf of which a telemarketing call is placed for calls answered during regular business hours. FCC also has a regulation prohibiting telemarketers from spoofing or blocking caller ID. FCC's regulation does not apply to tax-exempt nonprofit organizations, and it also allows telemarketers to transmit the name and customer service phone number of the seller on behalf of which a telemarketing call is placed. 47 C.F.R. § 64.1601(e).

[4]Consolidated Appropriations Act, 2018, Pub. L. No. 115-141, div. P, tit. V, § 503, 132 Stat. 348, 1091-94 (2018), codified at 47 U.S.C. § 227(e). DOJ has also made efforts to educate consumers about illegal spoofing; however, DOJ's consumer education efforts are outside of the scope of this review.

[5]The system is commonly referred to as STIR/SHAKEN or SHAKEN/STIR. STIR/SHAKEN are acronyms for the Secure Telephone Identity Revisited (STIR) protocol and the Signature-based Handling of asserted information Using toKENs (SHAKEN) framework.

The RAY BAUM'S Act of 2018 included a provision for us to review federal efforts to combat illegal spoofing.[6] This report examines:

1. what is known about caller ID spoofing schemes, including any recent trends;
2. FCC's, FTC's, and DOJ's enforcement efforts to combat such schemes;
3. FCC's and FTC's efforts to educate consumers about spoofing schemes; and
4. the status of industry efforts to develop technologies to combat spoofing, and FCC's role in these efforts.

To examine what is known about caller-ID-spoofing schemes and recent trends, we obtained and analyzed FCC and FTC consumer complaint data from January 2015 (when FCC launched a new portal for filing complaints) to December 2018 (the most recent month for which both agencies provided data), for the purpose of describing trends in consumer complaints related to unwanted and spoofed calls. We also obtained data from call blocking and analytics services to describe trends in unwanted and spoofed calls. We assessed the reliability of both sets of data by reviewing relevant documentation and conducting interviews with industry officials. We determined that these data were sufficiently reliable for our purposes. Additionally, we reviewed FCC and FTC documentation on caller ID spoofing and robocalls, including public notices and fact sheets and analyzed comments filed with FCC in response to relevant proceedings.

To examine FCC's, FTC's, and DOJ's enforcement efforts to combat schemes involving the use of caller ID spoofing, we reviewed and described enforcement cases brought by the agencies from April 2006 to June 2019 that involved the use of caller ID spoofing or blocking (the time period reflects the range of cases the agencies provided us). We also

[6]The provision required us to submit a report on the findings of our review to the relevant Congressional committees not later than 18 months after the date of enactment of the Act, which occurred on March 23, 2018. As agreed with committee staff, we met this requirement by submitting the draft report to the committees for informational purposes on October 21, 2019, when we also submitted the draft to the agencies for comment. The later submission date was agreed to in light of the federal government shutdown of 2018-2019. See Pub. L. No. 115-141, div. P, tit. V, § 503, 132 Stat. 348, 1091-94 (2018), codified at 47 U.S.C. § 227(e).

compared these agencies' efforts to collaborate on spoofing investigations and enforcements actions with seven practices for enhancing interagency collaboration that we identified in prior work.[7] Additionally, we assessed the agencies' descriptions—obtained from agency documents and interviews or written responses to questions—of how they prioritize their enforcement efforts against federal standards for internal control related to addressing risks.[8]

To evaluate FCC's and FTC's efforts to educate consumers about spoofing schemes, we interviewed agency officials, reviewed FCC and FTC educational materials, and compared these agencies' efforts to key practices for consumer education that we identified in our prior work.[9] We also compared these agencies' collaborative efforts to educate consumers to the same key practices for enhancing collaboration mentioned above.

To examine the status of industry efforts to develop technologies to combat caller ID spoofing, and FCC's role in these efforts, we reviewed FCC and industry documentation and compared FCC's efforts to federal guidance on how federal agencies should engage in standards activities.[10]

To address all our objectives, we reviewed relevant statutes and regulations, including the Telephone Consumer Protection Act of 1991

[7]See GAO, *Results-oriented Government: Practices that Can Help Enhance and Sustain Collaboration among Federal Agencies*, GAO-06-15 (Washington, D.C.: Oct. 21, 2005). We did not evaluate the agencies on one key practice identified in this report—reinforcing individual accountability for collaborative efforts through agency performance management systems—because it was out of the scope of this review, as our work did not incorporate an analysis of the agencies' performance management systems.

[8]GAO, *Standards for Internal Control in the Federal Government*, GAO-14-704G (Washington, D.C.: Sept. 10, 2014).

[9]GAO, *Digital Television Transition: Increased Federal Planning and Risk Management Could Further Facilitate the DTV Transition*, GAO-08-43 (Washington, D.C.: Nov. 19, 2007).

[10]Office of Science and Technology Policy, United States Trade Representative, Office of Management and Budget, *Memo on Principles for Federal Engagement in Standards Activities to Address National Priorities*, Memo M-12-08 (Washington, D.C.: Jan. 17, 2012).

and its provisions related to the use of robocalls;[11] the Telemarketing and Consumer Fraud and Abuse Prevention Act,[12] under which FTC issued regulations prohibiting deceptive and other abusive telemarketing acts or practices, including caller ID spoofing;[13] as well as the Truth in Caller ID Act of 2009. We interviewed agency officials from FCC, FTC, and DOJ. We also interviewed 23 nonfederal stakeholders, including representatives from industry associations, voice service providers, call blocking and analytics services, consumer groups, mobile phone manufacturers, and a standards body, as well as other knowledgeable stakeholders (see app. I for a list of stakeholders we interviewed). We identified these nonfederal stakeholders through our prior telecommunications work, other telecommunications reports, and recommendations from stakeholders we interviewed. While the views of the stakeholders we interviewed cannot be generalized, they provide valuable insight to our work. In addition, we interviewed officials from the Department of Homeland Security, which has undertaken efforts to address threats from caller ID spoofing, and the Department of the Treasury Inspector General for Tax Administration about the role of caller ID spoofing in scams involving the impersonation of the Internal Revenue Service (IRS).

We conducted this performance audit from May 2018 to December 2019 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Background

According to FCC, caller ID services became commonplace due to technology developed in the 1980s, and caller ID information transmitted with the call could generally be trusted by the call recipient. However, FCC found as voice service providers migrated to Internet Protocol (IP)

[11]Pub. L. No. 102-243, 105 Stat. 2394 (1991), codified at 47 U.S.C. § 227.

[12]Pub. L. No. 103-297, 108 Stat. 1545 (1994), codified at 15 U.S.C. §§ 6101-6108.

[13]The Telemarketing Sales Rule, 16 C.F.R. Part 310.

networks, these technologies lessened the overall accuracy and reliability of the information presented to the call recipient. Caller ID allows the recipient of an incoming call to determine the telephone number of the caller and, in some cases, the name. This information helps the recipient make informed decisions about which calls to accept or ignore. While the number and name displayed on the caller ID may be associated with the caller, a caller can also deliberately falsify or "spoof" the information transmitted to the caller ID display to disguise the source of the call. Under the current telephone system, this information, true or false, is conveyed to the call recipient unless the caller requests that such information not be conveyed.

Caller ID spoofing is widespread. Many instances of spoofing are legal. For example, spoofing is legally used by professionals such as doctors who want to use their cell phones to return calls to patients but choose to transmit their office number instead. Spoofing also often accompanies robocalls—an automated telephone call which delivers a recorded message. Certain types of robocalls are illegal, such as robocalls for sales pitches unless companies have consumers' express written permission to call.[14] In addition, telemarketers may not call home or mobile numbers that consumers have registered in the National Do Not Call Registry, which was established through legislation and is maintained by FTC—and they must transmit their telephone number and, if possible, their name, to the call recipient's caller ID.[15]

According to FCC, advancements in technology have made it inexpensive and easy to make robocalls.[16] As telecommunications systems have transitioned from traditional wireline services, to IP networks, the cost of

[14]47 C.F.R. § 64.1200. Some robocalls are permissible without a consumer's written or non-written consent, including certain calls to cell phones from debt collectors, health care providers, charities and candidates for public office.

[15]16 C.F.R. § 310.4(b). Exceptions to this include: political calls, survey requests, calls from non-profits and companies with whom the consumers have done or sought to do business over the last 18 months.

[16]In addition, some IP-based voice services allow individual callers to spoof caller ID by specifying the number they display as the caller ID using a web or mobile application. Caller ID spoofing services also advertise on the internet. Through a web interface or by calling the spoofing service's toll free number, the caller enters the number they wish to call, followed by the number they want to be displayed to the recipient.

making phone calls has dramatically decreased.[17] IP-based voice services use existing internet connections to send phone calls, which may be cheaper than long distance phone charges associated with traditional phone service. Autodialers can be programmed to dial a long list of phone numbers in order to deliver millions of calls in a short period of time. These dialing systems, coupled with IP-based voice services, such as Voice over Internet Protocol (VoIP),[18] enable telemarketers and scammers to make high volumes of calls from anywhere in the world.

IP-based voice services have also made it inexpensive and easy to spoof caller IDs. According to an industry stakeholder, historically, the router systems used to spoof calls were physical devices located on site, which could be prohibitively expensive. However, software that is available for free can now be downloaded to enable a computer to function as a router.[19] According to stakeholders, telemarketers and scammers can, with minimal cost, configure a router to display either a single spoofed number or a constantly changing set of numbers, making it appear as though calls originated in the United States even if they did not.[20] (See fig. 1.)

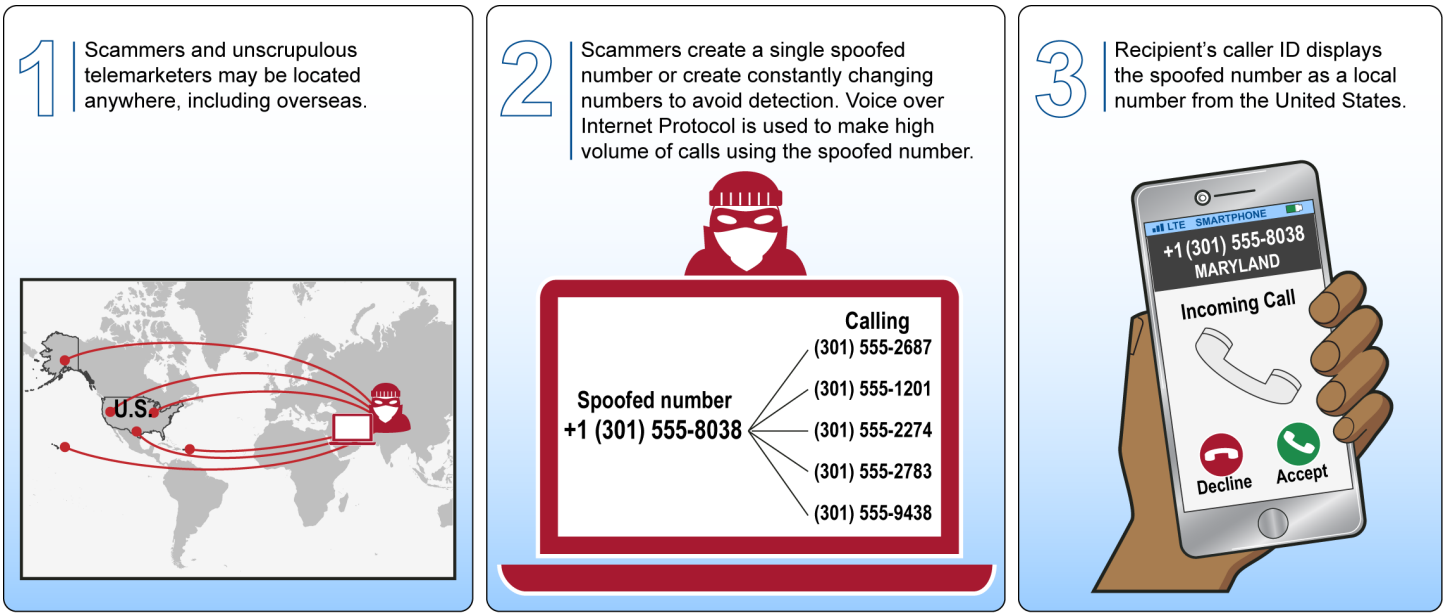
[17]IP networks route voice conversations over the Internet or any other IP network.

[18]VoIP is the routing of voice conversations over the Internet or any other IP network.

[19]FCC DA 11-1089 – Caller Identification Information in Successor or Replacement Technologies, June 22, 2011.

[20]In order to complete the call, the call is transferred from the Internet to a termination service located in the United States that serves as a gateway for transferring calls to the public switched telephone network, the interconnected network of telephone exchanges over which telephone calls travel from person to person.

Figure 1: How Caller ID Is Spoofed



Source: GAO analysis of Federal Trade Commission information. | GAO-20-153

FCC, FTC, and DOJ each enforce different rules or laws related to caller ID spoofing.[21]

- FCC enforces rules prohibiting anyone from causing the transmission of misleading or inaccurate caller ID information with the intent to defraud, cause harm, or wrongfully obtain anything of value.[22] FCC also enforces rules requiring telemarketers to transmit caller ID information.[23]
- FTC protects consumers against unfair or deceptive business acts or practices.[24] FTC, similar to FCC, enforces rules requiring

[21]Other federal and state agencies also have conducted investigations and taken enforcement actions against illegal use of spoofing when it relates to that agency's mission. These investigations and enforcement actions are not included in the scope of this report.

[22]47 U.S.C. § 227(e). 47 C.F.R. § 64.1604.

[23]47 C.F.R. § 64.1601(e).

[24]5 U.S.C. § 45.

telemarketers to transmit their telephone number, and when available, the name of the telemarketer to a consumer's caller ID service.[25]

- DOJ enforces federal fraud statutes under which fines or imprisonment can be imposed against anyone who uses interstate telecommunications as part of a fraud scheme.[26] DOJ can also take civil enforcement actions on FTC's behalf.[27]

FCC and FTC each manage consumer complaint databases where consumers can file complaints about unwanted calls, robocalls, and violations of the Do Not Call Registry.

In addition to government efforts, the telecommunications industry, including voice service providers and third party companies, have taken steps to counteract illegal spoofing. For example, some of these companies have developed or deployed applications (i.e., software programs, often referred to as apps) to defend against robocalls and other unwanted calls. This includes call blocking devices for landline telephones and various mobile applications that can label and block robocalls and other unwanted calls based on call patterns, consumer complaints or other means. While some carriers provide these services free, others may charge a fee. In addition, some carriers also work with analytics providers to analyze traffic on their networks. Beginning in 2017, FCC authorized voice service providers to block certain categories of unwanted calls before they reach consumers' phones.[28] Recently, FCC clarified that service providers can also, as a default, block calls identified

[25]16 C.F.R. § 310.4(a)(8).

[26]See e.g., 18 U.S.C. § 1343.

[27]FTC must notify DOJ of its intention to commence, defend, or intervene in any civil penalty action under the Federal Trade Commission Act. DOJ then has 45 days in which to commence, defend, or intervene in the suit. If DOJ does not act within the 45-day period, FTC may file the case in its own name, using its own attorneys. 15 U.S.C. §56(a)(1).

[28]*In the Matter of Advanced Methods to Target and Eliminate Unlawful Robocalls*, Report and Order and Notice of Proposed Rulemaking, 32 FCC Rcd 9706 (2017). This includes calls that appear to originate from (1) invalid numbers, such as area codes that don't exist (2) numbers that have not been assigned to a provider and (3) numbers that are assigned to a provider but not in use. In addition, service providers can block calls from numbers that are not used to place outbound calls, for example some government phone numbers.

as likely unwanted based on the provider's reasonable analysis of call data unless consumers opt out of this service.[29]

Caller ID Spoofing Is Used in a Variety of Financial Fraud and Other Schemes, and Consumer Complaints Suggest a Substantial Increase in Its Use

Caller ID Spoofing Schemes Seek to Obtain Money or Valuable Financial and Personal Information, Generate Telemarketing Leads, or Harass

Scammers use caller ID spoofing to facilitate a variety of financial fraud and other schemes, often in combination with robocalling. Based on our analysis of FCC, FTC, and DOJ enforcement cases and alerts from federal and state government agencies, as well as interviews with stakeholders, we identified three types of caller ID spoofing schemes.

- **To Obtain Money or Information:** Scammers have used caller ID spoofing to trick consumers into providing their financial or personal information or sending money such as via a debit or gift card. These scammers may spoof a name and phone number that looks familiar and trustworthy, such as that of a government agency, a company you do business with, or local number. Scams include telling call recipients they may be arrested or they owe money. For example, spoofed robocalls have been used as part of a wide-reaching scam in which callers spoofed IRS phone numbers and impersonated IRS staff to trick people into sending the scammers money for supposed unpaid taxes. IRS reported that from October 2013 through March 2019, the agency was contacted more than 2.4 million times by taxpayers who reported such calls, and more than 15,453 taxpayers reported losing about $75.1 million. (See fig. 2.)

[29]*See In the Matter of Advanced Methods to Target and Eliminate Unlawful Robocalls; Call Authentication Trust Anchor*, CG Docket No. 17-59, WC Docket No. 17-97, Declaratory Ruling and Third Further Notice of Proposed Rulemaking. 34 FCC Rcd 4876 (2019).

Figure 2: Internal Revenue Service Impersonation Scam

Source: GAO analysis of Federal Trade Commission information. | GAO-20-153

- **To Generate Telemarketing Leads:** Unscrupulous telemarketers have used spoofing as part of an attempt to sell goods or services. In this scheme, consumers may receive a pre-recorded robocall with a sales pitch and be instructed to "press 1" to indicate interest, at which point the call recipient is transferred to a live operator. In one such scheme, more than 96-million spoofed robocalls were made over a 3-month period.[30] These calls included pre-recorded messages falsely claiming to be from Hilton and other well-known travel companies; once consumers were transferred, live operators attempted to sell vacations not affiliated with the brands presented during the prerecorded message.
- **To Harass:** People have used spoofing to harass others. In some of these cases, people have used spoofing to cause another person's caller ID to display a familiar or trusted phone number. In one case, an individual apparently placed 31 spoofed calls as part of a personal campaign to harass and stalk another person.[31] These spoofed numbers appeared to be from the victim's child's school, among others. Spoofing is also one of several techniques used to place false calls to emergency response centers to elicit a police response to an address where no emergency exists. Callers have used spoofing to make it appear as if their call originated at or near the reported address. This practice, known as swatting, has resulted in death. For

[30]FCC Forfeiture Order FCC 18-58, May 10, 2018.

[31]FCC Forfeiture Order DA 17-57, January 13, 2017.

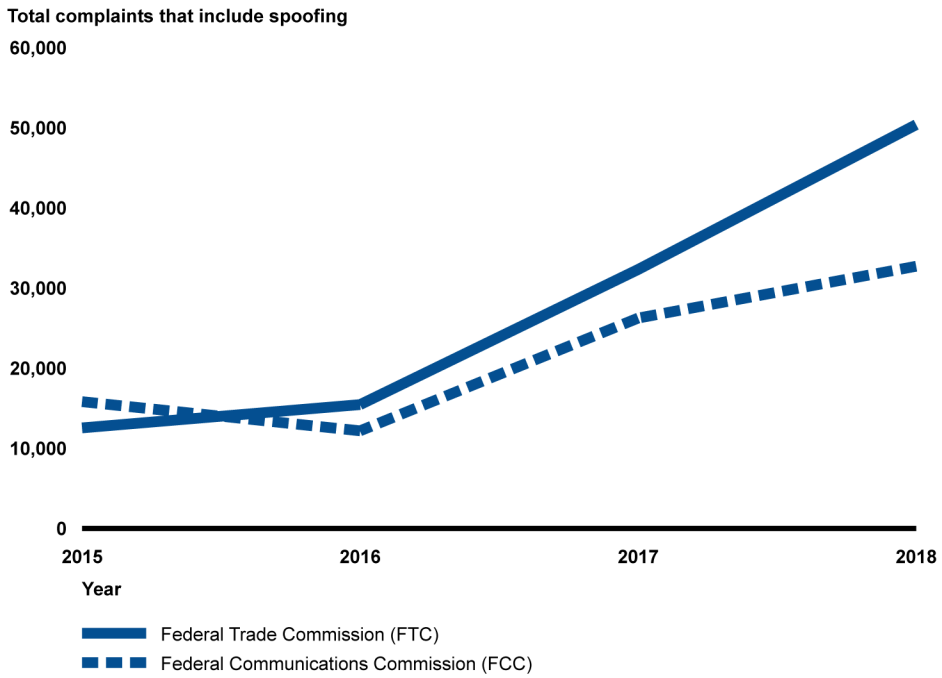
example, in one swatting case, a man was shot and killed by police who believed he was holding others at the address hostage.

Available Data Suggest That Caller ID Spoofing Is a Growing Issue

FCC and FTC consumer complaint data both show dramatic increases in recent years in the number of unwanted call complaints that specifically mention the term spoofing. According to our analysis of FCC and FTC complaint data, from 2015 through 2018, complaints to FCC that specifically referred to spoofing more than doubled and those received by FTC increased by more than four times.[32] (See fig. 3).

[32]Consumers submit complaints related to a wide array of unwanted calls. A detailed analysis of the narrative fields of these individual complaints is required to identify the nature of the complaint, including whether the consumer identified the call as having a spoofed caller ID. We analyzed FCC unwanted call data to identify those complaints that included the term “spoof” by month and year. FTC provided us with the number of unwanted call complaints that included the term “spoof” by month and year.

Figure 3: Consumer Complaints Submitted to FCC and FTC That Specifically Identified Spoofing, 2015 through 2018



Source: GAO analysis of FCC and FTC consumer complaint data. | GAO-20-153

Note: In 2018, complaints that specifically mentioned the term spoofing still represented a relatively small percentage of total unwanted call complaints—about 14 percent of FCC's total unwanted call complaints and about 1 percent of FTC's total complaints about unwanted calls. Spoofing is the practice of deliberately falsifying the information transmitted to the caller ID display to disguise the source of the call.

Table of Figure 3: Consumer Complaints Submitted to FCC and FTC That Specifically Identified Spoofing, 2015 through 2018

Agency	2015	2016	2017	2018
Federal Trade Commission (FTC)	12,550	15,456	32,317	50,386
Federal Communications Commission (FCC)	15,824	12,185	26,250	32,719

Examples of Consumer Complaint with Neighbor Spoofing

"This company relentlessly calls. They are using the caller ID of our local hospital. When they call, [the hospital's name] displays on the caller ID. I answer thinking they are calling to schedule for tests. They identify themselves, "hi this is Jennifer (names change) with BE SAFE AT HOME." I have asked them to stop calling. I am in the do not call registry. They won't stop! My biggest concern is the spoofing of our local hospital caller ID information."

"Rachel from Cardholder Services" has called me from local numbers for months. Today it hit a new low when I saw my caller ID had my mother's cell phone number. I answered only to hear this stupid RoboCall on a number they could not possibly be calling from. This caller uses "spoofing" and needs to be tracked down with more effort."

Source: FTC. | GAO-20-153

Several industry stakeholders we spoke with noted a growing trend in one particular type of spoofing, neighbor spoofing. Neighbor spoofing occurs when the caller ID is manipulated to display a phone number matching the area code and prefix (the first six digits) of the consumer's phone number. Consumers may be more inclined to answer these calls because they appear to be local—perhaps from someone they know.[33] Among FCC's complaints that included both the caller's and the call recipient's phone numbers, the percentage that were indicative of 6-digit neighbor spoofing increased from 10 percent in 2015 to 15 percent in 2018;[34] for similar FTC complaints, the percentage increased from 2 percent in 2015 to 16 percent in 2018;[35] and a call blocking provider told us that its percentage of neighbor-spoofed robocalls increased from 2 percent in January 2016 to 23 percent in December 2018.[36]

One analytics provider told us there has been a shift recently from spoofing the first six digits to spoofing the first four and five, which the provider believed to be a reflection of scammers adjusting their methods as more people become aware of the original six-digit form of neighbor spoofing. From 2015 to 2018, FCC and FTC data show substantial increases in complaints indicative of four and five digit neighbor spoofing, with FCC complaints nearly doubling and FTC complaints increasing more than 10 times during this time period.[37]

[33]While the caller's information may appear local, these calls may be placed by scammers or telemarketers who are located outside the state or country.

[34]FCC complaints indicative of 6-digit neighbor spoofing increased from 17,421 in 2015 to 30,018 in 2018.

[35]FTC complaints indicative of 6-digit neighbor spoofing increased from 67,845 in 2015 to 945,714 in 2018.

[36]FCC's complaint form includes a field that asks whether the complainant received caller ID information. If the complainant answers "yes," fields appear for the complainant to enter the caller ID number and name that were received. FTC's complaint form includes a field that asks for the phone number that received the call and the phone number that called the complainant.

[37]FCC complaints indicative of four and five digit neighbor spoofing increased from 37,348 in 2015 to 72,730 in 2018. Similar FTC complaints increased from 203,117 in 2015 to 2,425,337 in 2018.

FCC and prior GAO work[38] have described several limitations with using complaint data as a means of measuring the extent of unwanted calls.[39] For example, complaints might increase following consumer outreach regarding how to file a complaint or after news media coverage of a particular scam. In addition, not all consumers who experience problems file complaints, and not all complaints are necessarily legitimate or categorized appropriately. Further, a consumer could submit a complaint more than once, or to more than one agency, potentially resulting in duplicate submissions. Finally, while some consumers may use the term "spoof" when describing the complaint, others may not, either because they do not know they have been spoofed or are not familiar with the term. According to our analysis of FCC data, in 2018, 66 percent of all complaints that were indicative of neighbor spoofing did not include the term "spoof" in the complaint description.[40] Nonetheless, FCC, FTC, and DOJ officials told us they use this complaint data to identify specific trends in types of scams that may help the agencies' enforcement and public education efforts, which we discuss later in this report.

Although we could not find industry data that estimated the total number of spoofed calls, available industry data suggest that the volume of unwanted calls and robocalls (of which illegally spoofed calls are a subset) has increased over the past several years. Using call patterns on their own networks or other means, voice service providers, call blocking applications and analytics providers track data on unwanted calls and robocalls.[41] According to one company, these companies may have limited ability to detect or isolate spoofed calls, in part, because scammers may frequently change the numbers they use.[42] In addition, stakeholders told us, because each of these companies analyzes their specific user base and may use different methods to identify and label

[38]GAO, *Event Ticket Sales: Market Characteristics and Consumer Protection Issues*, GAO-18-347 (Washington, D.C.: Apr 12, 2018).

[39]FCC, *Report on Robocalls*, CG Docket No. 17-59, Feb. 1, 2019.

[40]We identified complaints that were indicative of neighbor spoofing, as previously described, and specifically identified spoofing.

[41]These companies analyze whether a call is likely to be an unwanted call or robocall based on call patterns on their networks and consumer complaints to FCC, FTC or the companies themselves.

[42]Scammers may rotate the numbers they are using to place calls every few minutes, making it difficult for the algorithms used by call blocking applications to identify them.

robocalls and other unwanted calls, the number of unwanted calls each company estimated may be substantially different. For example, while one analytics company estimated 26.3 billion robocalls nationwide in 2018, another company estimated the number at nearly 48 billion. Similarly, one company estimated a 46 percent increase in robocalls from 2017 to 2018, while another estimated a 57 percent increase for the same time period. Despite these differences, all analytics and call blocking companies we interviewed reported that their estimates of the number of unwanted calls and robocalls have increased in recent years.

Because there is no comprehensive data source on unwanted calls, robocalls, or spoofed calls, it is not possible to reliably estimate national trends. FCC has taken steps to seek input from industry and other stakeholders on how to better measure the extent of the unwanted call and spoofing problem. In a November 2017 Further Notice of Proposed Rulemaking, FCC sought comment on, among other things, what information should be collected to evaluate the effectiveness of efforts to combat these calls and whether FCC should adopt a reporting obligation for providers.[43] FCC received numerous comments from voice service providers, their associations, and other stakeholders in response to this notice. One commenter expressed concern that a reporting obligation would be burdensome to providers or of little benefit to FCC, and other commenters stated the agency should instead continue to monitor trends in consumer complaints. More recently, in a June 2019 Declaratory Ruling, FCC adopted a recommendation from 2017 to prepare two reports—one in 2020 and a second in 2021—to measure the effectiveness of efforts to combat illegal robocalls.[44] The ruling explicitly delegates authority to FCC staff to collect any and all relevant information and data from voice service providers necessary to complete these reports and states that the report should include authoritative data about the number of illegal robocalls.

Agencies Consider Risk of Harm to Public and Generally Follow Key Collaboration Practices in

[43]32 FCC Rcd 9706 (2017).

[44]34 FCC Rcd 4876 (2019). The reports are to be submitted to FCC no later than 12 and 24 months after the publication of this Declaratory Ruling and Third Further Notice of Proposed Rulemaking in the Federal Register, which occurred on June 24, 2019.

Their Enforcement Efforts, but Face Significant Challenges

Agencies Reported Taking Risk-Based Approach to Prioritizing Spoofing-Related Investigations and Enforcement Actions, but Collecting Evidence Can Be Difficult

FCC, FTC, and DOJ officials all said that their agencies must prioritize which illegal spoofing activity to investigate and take enforcement action against because they do not have sufficient resources to pursue all such activities. FCC and FTC officials stated that while they review complaint data and other information, it would not be practical to open investigations related to every complaint. According to officials at all three agencies, given their limited resources, the agencies prioritize investigations based on the level of harm being perpetrated and the likelihood of being able to effectively bring an enforcement case. Such prioritization is consistent with standards for internal control in the federal government. Those standards call for agencies to estimate the significance of risks to achieving agency objectives—in this case objectives related to protecting the public from harm—and to use those estimates as a basis for responding to the risks.[45] More specifically:

- In a 2015 letter to several members of Congress, the Chairman of the FCC stated that the agency is more likely to pursue enforcement action when a problem appears to be pervasive, represents a trend, involves an agency priority, affects many consumers, reflects particularly egregious abuse, or presents a security or safety concern.[46] Focusing specifically on investigations and enforcement action related to caller ID spoofing, FCC officials told us that the agency's three highest priorities are events that (1) threaten public safety; (2) involve very large numbers of spoofed calls; or (3) involve malicious scams or threats.

[45]GAO-14-704G

[46]Tom Wheeler, Chairman of the Federal Communications Commission, letter on the Federal Communications Commission's enforcement process to several members of the Senate's Committee on Commerce, Science, and Transportation, December 18, 2015.

- FTC's strategic plan for fiscal years 2018 to 2022 calls for the agency to target its enforcement efforts on those areas that cause the greatest amount of consumer harm. In line with this objective, FTC officials told us that the agency decides which consumer complaints to investigate based on the level of harm being perpetrated, as well as the likelihood of being able to effectively bring an enforcement case.
- DOJ's *Justice Manual* states that serious violations of federal law must be prosecuted.[47] DOJ officials told us that for fraud schemes that employ caller ID spoofing, the agency is more likely to charge a violation of one of the fraud statutes, such as mail fraud, wire fraud, computer fraud, or conspiracy, as well as the money laundering and identity theft statutes.[48] Specifically with regard to wire and mail fraud cases, the *Justice Manual* states that serious consideration should be given to the prosecution of any scheme which in its nature is directed to defrauding a class of persons or the general public with a substantial pattern of conduct.

FCC and FTC officials stated that there are significant challenges related to investigating spoofing cases that can affect which investigations they choose to pursue and limit the number of enforcement cases they are able to bring. For example, FTC officials stated that the use of VoIP technology enables fraudsters to easily change both their physical locations and the numbers they spoof, making it harder for FTC and other law enforcement agencies to track them down. An industry stakeholder said that the use of VoIP technology makes it difficult to determine even whether the call originated domestically or from overseas. Moreover, FCC officials stated that when spoofed calls originate wholly from a foreign jurisdiction, a lack of foreign cooperation can make it exceptionally difficult to follow a trail back to either the service provider that originated the call or the person or company making the calls. The officials explained that foreign cooperation may be lacking when the calls come from countries with which the United States does not have strong diplomatic relationships. The officials stated that because of this challenge, they are less likely to bring an enforcement case when calls originate wholly from a foreign jurisdiction, due to the low likelihood of successfully resolving

[47]Department of Justice, *Justice Manual.* Title 9 Criminal, Principles of Federal Prosecution Selecting Charges — Charging Most Serious Offenses, 9-27-300 (updated February 2018).

[48]Department of Justice, *Justice Manual,* Title 9 Criminal, Policy Relating to Mail Fraud and Wire Fraud. 9-43.100 (updated April 2018).

such cases and the heightened use of limited staff resources required by such cases.[49]

Regardless of these challenges, FCC and FTC officials stated that their agencies have taken steps to improve their ability to investigate cases based overseas. For example, both agencies cited their outreach to the Indian government and the U.S.-India Business Council as well as their participation in the Unsolicited Communications Enforcement Network, a global network of law enforcement authorities and regulatory agencies that works to combat unsolicited communications.

FCC, FTC, and DOJ Identified 62 Spoofing or Caller-ID-Blocking-Related Enforcement Cases Brought since 2006

FCC, FTC, and DOJ officials identified 62 enforcement cases that they said involved spoofing or blocking of caller ID information, though DOJ officials stated that their list of enforcement cases was not comprehensive because DOJ's enforcement database does not include an indicator for whether spoofing was employed as part of a fraud scheme.[50] (For a description of these 62 cases, see app. II.) As noted below, these 62 cases are not representative of all of the cases the agencies have brought related to illegal robocalling.

- FCC officials provided us information on six cases—each of which the officials said involved spoofing or a caller's blocking of their caller ID information—that the agency brought from April 2011 to September 2018.[51] For example, one case involved a company that used spoofed

[49]In August 2019, FCC amended its Truth in Caller ID rules to prohibit caller ID spoofing directed at the United States from callers outside the country, The prohibition becomes effective February 5, 2020. See 47 C.F.R. § 64.1604.

[50]DOJ officials stated that the agency identified its cases based on current staff knowledge. During the course of our review, we identified several additional DOJ cases that involved caller ID spoofing that were not on DOJ's list. Each of those cases also involved swatting. We did not attempt to identify all DOJ spoofing cases.

[51]FCC refers to these cases as *forfeiture actions*; a monetary forfeiture is a fine. According to FCC officials, in two of the cases FCC considered spoofing or blocking of caller ID information in apparent violation of its regulations when setting the fine amounts. However, according to the officials the fines FCC assessed in those two cases were for violations of the agency's rules prohibiting unsolicited prerecorded advertising calls. The officials said the other four cases involved spoofing and cited violations of the Truth in Caller ID Act of 2009.

robocalls to target elderly and low-income individuals to generate sales of health insurance coverage. The company's high numbers of robocalls also disrupted an emergency medical paging service. FCC issued fines in five of these cases, and one pending case includes a proposed fine. FCC officials told us that since January 2004, the agency has initiated approximately 20 additional enforcement cases and has issued approximately 1,000 warnings, all for robocalling or Do-Not-Call violations under the Telephone Consumer Protection Act of 1991.[52]

- FTC officials provided us information on 31 cases—each of which the officials said involved spoofing—that FTC brought—or that DOJ brought on FTC's behalf—from April 2006 to June 2019.[53] Examples of cases include several involving numerous calls to numbers on the National Do Not Call Registry and an incident in which a company impersonated government officials and help centers to make a sales pitch with false and misleading claims about an English-language learning course to Spanish-speaking U.S. consumers. Monetary judgments were issued in all but one of these cases. FTC officials told us that as of November 2019 the agency had brought 147 enforcement cases against Do Not Call and robocall violators. FTC officials also stated that FTC obtains injunctive relief in their Do Not Call, robocall, and spoofing cases, including court orders prohibiting the defendants from engaging in similar conduct, and in some cases, banning defendants from any telemarketing activity. Further, they stated the injunctive relief also includes reporting and compliance requirements to help FTC monitor defendants. FTC officials told us that the agency has obtained injunctive relief in all of its completed spoofing cases and that these injunctions provide strong deterrence and help stop illegal spoofing.

[52]47 U.S.C. § 503(b)(5). As described later in this report, under the Communications Act as it applies to the Telephone Consumer Protection Act of 1991, in many instances FCC must warn a party of its apparent violations and can only proceed with a monetary penalty if the party subsequently commits the same type of violation. The Communications Act refers to such warnings as *citations*.

[53]According to FTC officials, in each case FTC alleged that defendants failed to transmit complete and accurate caller ID information in violation of 16 C.F.R. § 310.4(a)(8) or assisted others in doing the same. FTC is required to refer all cases involving civil penalties to DOJ, which then has 45 days to bring the case on FTC's behalf. See 15 U.S.C. § 56(a)(1). If DOJ elects not to bring the case, FTC can then bring the case itself. Of the 31 cases, FTC brought 20 and DOJ brought 11.

- DOJ officials provided us information on 25 cases—each of which the officials said involved spoofing—that the agency brought from May 2010 to August 2018. Several of these cases involved companies or individuals that used spoofing as part of a scheme to swindle money from people. For example, in one case, defendants used spoofing as part of a scheme to defraud and extort money from victims who were falsely told they had failed to accept and pay for products they had never ordered. Twenty cases had judgments that included prison time; 18 cases had monetary judgements.

FCC and FTC have collected far less than has been assessed in fines or monetary judgements, but officials at both agencies stated that the amounts they have collected still serve both punitive and deterrent purposes.[54] Specifically, FCC officials stated that thus far, FCC has collected $25,970 of the approximately $205 million in fines it assessed. This mostly represents full payment of a $25,000 fine FCC issued in January 2017, but FCC has yet to collect any portion of the more recent fines it has issued: a fine of $120 million it issued in May 2018 and a fine of approximately $82 million it issued in September 2018. FCC has referred both of these cases to DOJ for collection action.[55] FCC officials noted that these large fines may not represent the amount that the defendants are able to pay, and that even payment of a fairly small fraction of a large fine could be enough to put a scammer out of business and serve as a substantial deterrent.

FTC officials said that FTC has obtained a total of about $363 million in monetary judgments in its 31 spoofing cases. The officials said that many of these judgements were partially suspended based on the defendants' ability to pay determined by a defendant's net worth and assets. Further, the officials said if the defendant misrepresents his or her financial position, the entire judgment can become due under a clause that is part of the judgement. The officials said that as of August 14, 2019, FTC had collected about $31 million in its spoofing cases, and that this amount

[54]FCC assesses civil penalties, whereas FTC seeks monetary judgments in cases it brings in federal court.

[55]FCC officials told us when a party fails to pay a fine, the case is referred to DOJ for collection action, and DOJ decides whether it will pursue the case–though DOJ often settles these cases. They further stated that when a party pays some but not all of a fine, the case is referred to Treasury for collection.

represents all or substantially all of the unsuspended judgments in those cases.

Officials with DOJ's Consumer Protection Branch said that the branch views monetary judgments as one piece of the deterrence equation for caller-ID-spoofing offenses. The officials stated that the low amounts collected suggest that other preventative measures, such as injunctive relief and imprisonment, must be employed to deter continued unlawful activity.

FCC, FTC, and Others Have Proposed Various Legal Changes to Strengthen Enforcement against Illegal Spoofing and Robocalling

FCC and FTC both favor some changes to law to enhance the effectiveness of their enforcement efforts. Specifically:

- In May 2019, FTC officials testified that the agency's enforcement efforts are hindered by a statutory provision that prohibits the agency from taking action against telecommunications carriers, to the extent they are engaged in common carriage activities.[56] FTC further testified that it would like this provision removed so that the agency could take enforcement action against carriers engaged in illegal telemarketing activities.
- In 2018, an FCC official publicly stated that a longer statute of limitations for enforcement of the Telephone Consumer Protection Act of 1991 would improve the agency's enforcement efforts against knowing and willful violators of the act. Currently, that act has a 1-year statute of limitations, while the Truth in Caller ID Act of 2009 has a 2-year statute of limitations.[57] FCC officials told us that harmonizing the two acts' statutes of limitations to 2 years would help FCC's

[56]15 U.S.C. § 45(a)(2).This statutory provision applies to telecommunications carriers, which are one type of voice service provider. While the Federal Trade Commission Act generally empowers FTC to take enforcement action against companies for unfair and deceptive trade practices, it prohibits FTC from taking action against common carriers such as telecommunication carriers, airlines, and railroads. Common carriers are generally entities that provide essential services that can be solicited by the general public.

[57]47 U.S.C. § 503(b)(6) and 47 U.S.C. § 227(e)(5)(A)(iv).

enforcement efforts since spoofing often occurs with robocalling and the agency often uses the two statutes in tandem.

- A February 2019 FCC staff report on robocalls notes that FCC's enforcement efforts can be hindered by the requirement that in many instances FCC must warn a party of apparent robocalling violations and can only proceed with a monetary penalty if the party subsequently commits the same type of violation,[58] a requirement in the Communications Act that applies to the Telephone Consumer Protection Act of 1991.[59] According to the report, this requirement enables a warned offender to incorporate under a new name to evade further detection and begin illegal activity anew. In contrast, the report notes, the Truth in Caller ID Act of 2009 allows FCC to directly issue a proposed monetary penalty without first issuing a warning.[60] Similar to the statutes of limitations just discussed, FCC officials told us that since spoofing often occurs with robocalling and the agency often uses the two statutes in tandem, their enforcement efforts would benefit from the elimination of this statutory requirement.

In 2019, bills were introduced in Congress that, if passed, would implement the changes in law that FCC and FTC have recommended and could potentially help address other challenges faced by FCC and FTC. For example, in July 2019, a bill was introduced in the Senate that would remove the provision prohibiting FTC from taking action against common carriers.[61] Also in 2019, two different bills were introduced, one in the House and one in the Senate, that would, among other things, address issues with harmonization of the FCC statute of limitations and eliminate the FCC pre-penalty warning requirement with respect to illegal robocalling.[62] In addition, one of these bills, the Telephone Robocall Abuse Criminal Enforcement and Deterrence Act (TRACED Act), would require DOJ, in consultation with FCC, to assemble an interagency working group to study and report to Congress on how to enhance enforcement against robocalls by examining issues like the types of laws,

[58]FCC, *Report on Robocalls*, CG Docket No. 17-59, Feb. 2019.

[59]47 U.S.C. § 503(b)(5). The Communications Act refers to such warnings as *citations*.

[60]47 U.S.C. § 227(e)(5)(A).

[61]Protection from Robocalling Act, S. 2349, 116th Cong. (2019).

[62]Telephone Robocall Abuse Criminal Enforcement and Deterrence Act (TRACED Act), S. 151, 116th Cong. (2019) and Stopping Bad Robocalls Act, H.R. 3375, 116th Cong. (2019).

policies, or constraints that could be inhibiting enforcement of the Truth in Caller ID Act of 2009. The interagency working group would also be tasked with identifying existing and potential international policies and programs that could encourage and improve coordination between countries. We have reported in past work that collaborative mechanisms such as interagency working groups can help the federal government achieve many of the meaningful results it seeks to achieve, and that such mechanisms all benefit from certain key features, which raise issues to consider when implementing these mechanisms.[63] As of November 2019, no federal legislation had been enacted on these issues.

Agencies' Efforts to Collaborate on Enforcement Efforts Generally Align with Key Practices

We found that FCC's and FTC's efforts to collaborate on spoofing investigations and enforcement actions align with seven key practices we have previously identified to enhance and sustain interagency collaboration.[64] FCC and FTC officials explained that their close collaboration helps ensure that they share relevant information and avoid duplicating efforts. In addition, we found that DOJ's collaboration with FCC and FTC aligns with five of the seven key practices. Although we did not find evidence that DOJ had taken steps in line with the other two key practices, officials at all three agencies stated that DOJ's collaborative efforts were appropriate given its broader jurisdiction and wider focus.

More specifically, we found that all three agencies have incorporated five key practices. Our prior work has found that one way agencies can incorporate three of these practices — (1) defining and articulating a common outcome, (2) establishing mutually reinforcing or joint strategies, and (3) agreeing on roles and responsibilities—is through a memorandum of understanding.[65] In 2003, FCC and FTC agreed to a memorandum of

[63]These key features include the categories of outcomes and accountability, bridging organizational cultures, and clarity of roles and responsibilities, among others. See GAO-12-1022.

[64]GAO-06-15.

[65]In GAO-12-1022, which highlights key features of collaborative mechanisms, we note that these three collaboration practices all relate to the key feature of clarity of roles and responsibilities. Roles and responsibilities can be clarified in a variety of ways, including in laws, policies, and memorandum of understanding.

understanding that calls for the agencies to cooperate and coordinate to implement consistent, comprehensive, efficient, and non-redundant enforcement of federal telemarketing statutes and rules. The memorandum also calls for the agencies to meet quarterly to discuss matters of mutual interest, share consumer complaints, and engage in joint enforcement actions when necessary. Consistent with the memorandum, FTC officials told us that FTC and FCC hold quarterly meetings to discuss how they are targeting robocalls and spoofing investigations and enforcement cases to avoid duplication. FTC and FCC officials stated that in addition, their collaboration with DOJ is enhanced through the participation of all three agencies in a monthly conference call hosted by the National Association of Attorneys General to coordinate efforts to combat illegal robocalls across the government.

Although DOJ officials told us that DOJ does not have a memorandum of understanding with FCC or FTC regarding spoofing or robocall-related enforcement, officials we interviewed at all three agencies identified collaborative efforts that DOJ engages in that are consistent with the three key practices cited above. FCC and DOJ officials stated they are developing procedures to share information on a particular enforcement case, and that these procedures could be used on other cases as needed in the future.[66] In addition, officials from all three agencies stated that DOJ's participation in the monthly conference calls and additional informal outreach as needed was sufficient to ensure effective collaboration.

With regard to the fourth and fifth key practices (4) identifying and addressing needs by leveraging resources, and (5) establishing compatible policies, procedures, and other means to operate across agency boundaries, FCC and FTC officials described regularly sharing information from their complaint databases, which is in line with these practices. FTC officials stated they regularly review FCC's complaint information to help their enforcement efforts. Moreover, FTC has established policies and procedures whereby DOJ and FCC and other law enforcement entities have access to FTC's complaint database, and FCC and DOJ officials stated that they frequently analyze FTC's complaint database to inform their investigative decisions. Furthermore,

[66]FCC officials said that the procedures will be consistent with FCC's regulations on the agency's disclosure to other federal agencies of information submitted to FCC in confidence. 47 C.F.R. § 0.442.

DOJ officials stated that DOJ recently contributed funds to FTC to enhance capabilities to analyze the database. FCC and FTC have also leveraged resources by co-hosting a public event in 2018 on reducing robocalls and spoofing that included discussions of recent policy changes and enforcement actions to stop illegal robocalls.

We found that FCC and FTC follow two additional key practices for collaborating on spoofing-related investigations and enforcement actions that DOJ does not: (1) developing mechanisms to monitor, evaluate, and report the results of collaborative efforts, and (2) reinforcing agency accountability for collaborative efforts through agency plans and reports. For example, FCC and FTC collaborated on a robocall report published by FCC in 2019 that discussed both agencies' enforcement actions related to robocalls and spoofing, and each discussed their collaborative efforts related to robocalls in key agency documents related to accountability and performance.[67] DOJ officials stated that they would be unlikely to have such materials specifically related to spoofing given the agency's focus on fraud itself rather than spoofing or robocalling, which it views as a means to fraud. DOJ officials stated that DOJ's general commitment to interagency collaboration is emphasized in its fiscal year 2020 budget submission to Congress and many press releases related to its enforcement cases. We reviewed DOJ's budget submission and several DOJ press releases and found that they mention collaboration between DOJ and other agencies.

[67]Specifically, FCC included a performance target in its fiscal year 2020 performance plan to work with other federal agencies on combatting unlawful robocalls, and FTC discussed the event that it co-hosted with FCC in its fiscal year 2020 budget justification.

FCC and FTC Have Robust Consumer Education Efforts That Follow Key Practices for Consumer Education and Interagency Collaboration

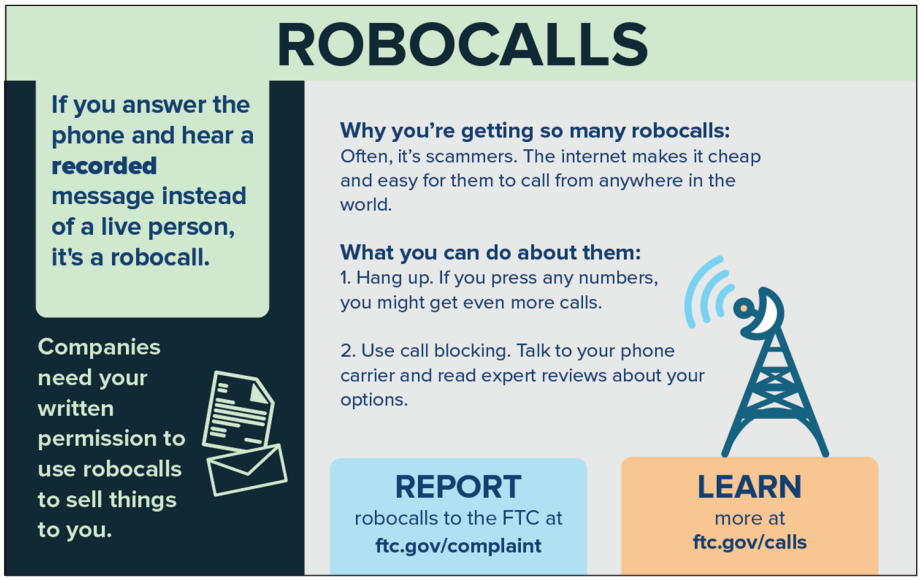
FCC and FTC use a number of methods to educate consumers on ways to protect themselves against spoofed and other unwanted calls.[68] According to FCC documentation, the agency has made combatting illegal robocalls and caller ID spoofing its top consumer protection priority and uses consumer education as a means to address this priority. Similarly, according to FTC's chairman, consumer education is a critical element of FTC's efforts to fulfill its consumer protection mission. The methods that FCC and FTC use—both independently and collaboratively—to educate consumers on ways to combat caller ID spoofing and unwanted calls include the following.

- **Posting online consumer alerts, videos, blog posts, and other informative materials:** Both FTC and FCC post information and warnings about caller ID spoofing scams on their websites. FTC, for example, developed Pass It On, a print- and web-based campaign to educate seniors about various types of scams that target seniors, including spoofing. FCC launched an animated video initiative on how to avoid spoofing scams and also posted a consumer alert about neighbor spoofing scams. The alert explains that scammers use such spoofing to increase the likelihood that consumers pick up the phone and provides tips such as to not answer calls from unknown numbers and to not provide any personal information to such callers. Additionally, FCC and FTC post other information, including tip cards and graphics such as those illustrated in figure 4.
- **Visiting vulnerable communities**: FCC has conducted speaking tours, such as tours through rural Appalachia and the Pacific

[68]DOJ also performs consumer outreach as part of its mission. DOJ officials described consumer outreach efforts that could include information related to spoofing—such as their broad outreach efforts to help prevent elder fraud and the media attention often resulting from these efforts that the officials said are sometimes referred to as "major take downs;" moreover, DOJ has published information on its website referring people to FTC's materials related to unwanted calls. However, because DOJ's focus as it relates to spoofing is on fraud, we did not assess DOJ's specific public education efforts related to spoofing in this report.

Northwest in 2018 to educate communities about spoofing, and to build partnerships to help improve the effectiveness of future outreach efforts. Similarly, FTC has hosted briefings in underserved communities with law enforcement, consumers, and community advocates to place more attention on consumer protection issues such as spoofing and other types of fraud.

Figure 4: FCC's Tip Card and FTC's Graphic to Educate Consumers on How to Avoid Spoofing and Robocalls



Source: Federal Communications Commission (FCC) and Federal Trade Commission (FTC). | GAO-20-153

We found that FCC's and FTC's consumer education efforts related to spoofing and other unwanted calls aligned with nine key practices for consumer education that we identified in our prior work (see table 1).[69] For example, FCC and FTC have developed consistent and clear consumer education messages related to spoofing and unwanted calls: specifically, consumers:

- should not answer unknown calls;
- should not push any numbers if directed to do so; and
- should hang up immediately once it is clear that the caller is unknown.

In addition, FCC and FTC officials have worked with credible messengers to help disseminate consumer education messages, including to potentially vulnerable populations. For example, since 2017, FCC has worked with the National Asian American Coalition to train grassroots volunteers to engage local community members and distribute educational tip cards printed by FCC in languages such as Mandarin Chinese, Korean, Vietnamese, and Tagalog. In addition, FTC has collaborated with AARP to develop three videos for Asian American and Pacific Islander communities on robocall, IRS, and Medicare scams.

[69]See GAO, *Digital Television Transition: Increased Federal Planning and Risk Management Could Further Facilitate the DTV Transition*, GAO-08-43 (Washington, D.C.: Nov. 19, 2007). In this 2007 report, we convened a panel of 14 experts representing public, private, and academic organizations to identify key practices for conducting consumer education. This panel came up with nine key practices.

Table 1: Assessment of Whether FCC and FTC Consumer Education Efforts Related to Unwanted Calls Align with Relevant Key Practices

Key practice	FCC's effort	GAO's assessment of FCC's effort	FTC's effort	GAO's assessment of FTC's effort
1. Define goals and objectives	FCC's FY 2020 Performance Plan contains a performance goal and related targets to seek out and eliminate unlawful telemarketing and robocalling.	Agency's actions align with key practice	Efforts to combat unwanted calls (that may include spoofing) are included under FTC's strategic goal and objectives to prevent fraud, deception, and unfair business practices in the marketplace.	Agency's actions align with key practice
2. Analyze the Situation	FCC officials stated they review materials from other government agencies, industry, and consumer-related non-profit organizations.	Agency's actions align with key practice	FTC officials said they work with agency attorneys to bring cases and review website page-views and consumer complaints.	Agency's actions align with key practice
3. Identify Stakeholders	FCC has identified and engaged stakeholders including federal, local, and private entities, to educate consumers about unwanted calls.	Agency's actions align with key practice	FTC has identified and engaged stakeholders including federal and local entities to educate consumers about unwanted calls.	Agency's actions align with key practice
4. Identify resources	FCC officials said they assess and budget for resource needs, such as staffing and printed materials, and continue to plan funding for consumer-education-related travel.	Agency's actions align with key practice	FTC officials said they continually assess staffing needs and use the Bureau of Consumer Protection's consumer education budget to pay for efforts to educate consumers about unwanted calls.	Agency's actions align with key practice
5. Research target audience	FCC officials said efforts to research target audience include collecting feedback from consumers and reviewing peer research studies to inform their educational content.	Agency's actions align with key practice	FTC officials said efforts to research target audience include reviewing consumer complaints and information from Foresee, a general survey on FTC's website.	Agency's actions align with key practice
6. Develop consistent, clear message	FCC's message to consumers is consistent and clear: Do not answer unknown calls, and, if you do, hang up.	Agency's actions align with key practice	FTC's message to consumers for combatting illegal robocalls is consistent and clear: Do not answer calls from unfamiliar numbers, and, if you do, hang up.	Agency's actions align with key practice
7. Identify credible messenger(s)	FCC officials work with entities such as AARP and the National Asian American Coalition to educate members about protecting themselves against illegal caller ID spoofing.	Agency's actions align with key practice	FTC officials told us that they work with entities such as AARP and libraries to get their message out to consumers about how to avoid unwanted calls.	Agency's actions align with key practice
8. Design media mix	FCC officials said they focus on earned media (such as news stories or opinion editorials). Since 2018, for example, over 1,375 articles mentioned FCC and "spoofing," and officials noted that potential audience reach from all media was over 2 billion.	Agency's actions align with key practice	FTC officials said they use media such as the agency's website, social media, and participating local-access cable television outlets to help distribute their message.	Agency's actions align with key practice

9. Establish metrics to measure success	FCC has established one measure, which is to reach 1-million consumers to identify and combat unlawful telemarketing and robocalls. FCC officials say steps to track progress toward this goal will include monitoring number of website visits, webinar participants, and email recipients.	Agency's actions align with key practice	FTC has established quantifiable output measures for its higher-level effort to protect consumers from unfair and deceptive practices in the marketplace.	Agency's actions align with key practice

Source: GAO analysis of Federal Communications Commission (FCC) and Federal Trade Commission (FTC) documents and interviews. | GAO-20-153

In addition, we found that, similar to their enforcement efforts, FTC and FCC's efforts to collaborate on public education in this area are consistent with the seven key collaboration practices we discussed earlier in this report. For example, FCC and FTC agreed to a second memorandum of understanding in 2015 that states that the agencies will collaborate with each other on consumer and industry outreach and education efforts, as appropriate. FCC and FTC also collaborate with other entities, including federal, local, and private entities, to educate consumers on ways to combat spoofing. For example, FCC officials told us that beginning in October 2018, they collaborated with Department of Veterans Affairs officials to send out three joint emails (from November 2018 through March 2019) to veterans and veterans' organizations on ways to protect themselves against illegal robocalls, including spoofed calls. These officials also noted that each email reached approximately 5.5 million targeted recipients.

Industry-Led Technical Effort to Reduce Spoofing Is Moving Forward, with FCC's Support in Line with Federal Guidance

Some Providers Are Deploying a Caller ID Verification System with a December 2019 Implementation Target

According to officials with industry groups, voice service providers, and FCC, the voice service provider industry has taken key steps towards successfully putting in place a caller ID verification system throughout much of the IP-based U.S. telephone network by the end of 2019. As discussed previously, the system is commonly referred to as

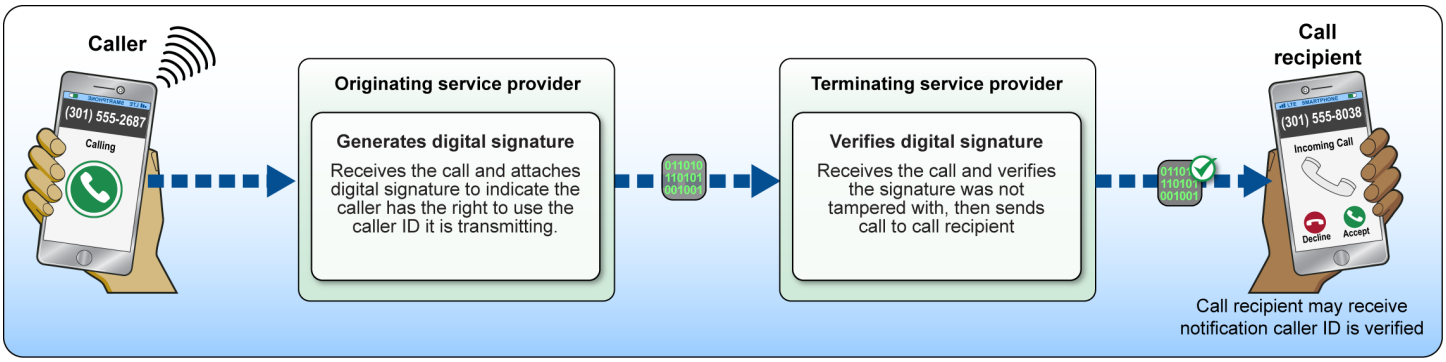
STIR/SHAKEN or SHAKEN/STIR.[70] According to the Alliance for Telecommunications Industry Solutions (ATIS), which spearheaded this industry-led effort along with the Session Initiation Protocol (SIP) Forum, the system is intended to enable voice service providers to verify that a caller has a right to use the caller ID transmitted with the call.[71] Under the system, the voice service provider that first initiates the call onto the network (originating service provider) generates a digital signature that attaches to the phone call indicating that the caller has this right. This occurs only when the originating provider knows this information and is considered the highest level of verification, referred to by the industry as "attestation."[72] The signature is transmitted along with the call as it is routed from one service provider to another. The terminating service provider, which passes the call onto the call recipient, can verify that the signature was not tampered with before sending the call to the call recipient (see fig. 5).

[70]STIR/SHAKEN are acronyms for the Secure Telephone Identity Revisited (STIR) protocol and the Signature-based Handling of asserted information Using toKENs (SHAKEN) framework.

[71]The mission of ATIS, an information and communications technology industry group, is to enhance collaboration and share resources, efforts, and costs to develop large-scale interoperable solutions for the common industry good. The caller ID verification system, developed by ATIS and the SIP Forum, is based on an internet protocol developed by the Internet Engineering Task Force. The SIP Forum is an industry association with members from IP communications companies. Its mission is to advance the adoption and interoperability of IP communications products and services based on SIP.

[72]According to ATIS officials, the digital signatures are based on common public key cryptography techniques. As described later in the report, the originating provider does not always know this information, and so the system includes lower levels of verification that the originating provider can attest to in these cases.

Figure 5: Schematic of System Being Deployed by Providers to Verify Caller ID Information



Source: GAO analysis of the Alliance for Telecommunications Industry Solutions information. | GAO-20-153

According to an FCC Notice of Proposed Rulemaking, as of June 2019, several major providers had deployed or were in the process of deploying the system on their own networks, and a few had started exchanging signed calls with a second provider.[73] In addition, ATIS has announced a number of key steps taken to fully implement the system's framework. For example, in September 2018, ATIS launched the system's governance authority, whose board consists of representatives from a variety of U.S. voice service providers and relevant industry associations, and which, according to ATIS, is overseeing the system to ensure that it is effective and secure. In August 2019, ATIS issued a press release stating that the governance authority board had determined the requirements service providers must meet in order to get certificates to digitally sign calls and had contracted a private firm tasked with ensuring that only authorized service providers get these certificates. According to an industry official who worked on this effort, once most U.S. carriers deploy the system and are sharing information across their networks, the technical experts who developed the standards will be able to see how it works and improve and enhance the system through additional technical developments.

Because it is not always possible for the originating service provider to determine whether the caller has a right to use the phone number that will be displayed, in addition to the top level of verification, the system was designed with a middle level and a lowest level of verification. The originating service provider digitally signs the call with the middle level of attestation when the provider has an established relationship with the

[73]34 FCC Rcd 4876 (2019).

caller but does not know whether the caller has the right to use the phone number it will display. According to ATIS officials, the originating service provider may use this level of attestation, for example, when a call comes from a corporate call center, which displays all outbound calls as originating from a central number or set of numbers. The originating service provider signs the call with the lowest level of attestation when it is responsible for originating the call onto its network but it does not have a relationship with the caller (such as when the call comes in from another country). When using either the middle or lowest level of attestation, the provider cannot determine if the call is spoofed. However, according to ATIS officials, the information that provided the basis for the attestation level is still likely to be helpful. For example, this information may better position the terminating service provider or call blocking and analytics apps to determine, in combination with other data the terminating service provider or such apps may have analyzed, whether to block or warn the consumer about the call.[74]

According to officials from several carrier associations or voice service providers, the new system should substantially improve the industry's ability to combat spoofing and block unwanted calls by providing carriers with immediate verification information. These stakeholders, as well as FCC officials, also stated that enabling voice service providers to instantly identify the provider that initiated the call onto the network—through the digital signature attached to the call— could help facilitate federal investigations by accomplishing in an instant what can now take significant time and effort as the call must be traced back from provider to provider. One stakeholder who played a key role in the development of the system stated that as some U.S. service providers deploy this system and more calls are able to be verified, it is likely to incentivize other U.S. providers to deploy verification systems so that their calls will not stand out as unverified. This stakeholder said that the hope is that other countries, including those with many legitimate call centers that send calls to the United States, such as India, will also implement verification systems that eventually can be integrated with the U.S. system. And as more calls are able to be verified, the stakeholder explained that the system will become more valuable and useful.

[74]For example, a terminating service provider could choose to provide a green check, the word "verified," or any other indication next to a verified number. Similarly, a terminating service provider determines how to indicate that a call has not been or cannot be verified.

An ATIS representative and other stakeholders identified other examples of ongoing technical challenges and open issues:

- **Information provided to consumers:** The industry has not reached agreement about what, if any, information should be presented to call recipients to inform them that the call has or has not been verified.[75] Stakeholders we spoke with noted that it is important to educate consumers on the limitations of any such information. For example, although a call may be verified, the provider cannot guarantee that the caller is not trying to defraud the call recipient—just that the caller is not using a spoofed phone number to do so. Further, if a provider is unable to verify the caller ID information, it does not necessarily mean the call is fraudulent or the caller has malicious intent. For these reasons, several industry stakeholders we spoke with emphasized that the information provided by this system can be most useful when combined with other methods service providers use to analyze call traffic to identify unwanted or illegal calls.
- **IP-only system:** Several stakeholders also emphasized that the system only works for calls carried entirely over IP networks, not those using traditional wireline networks. One industry group representing smaller providers that may use traditional wireline networks expressed concerns that its members may need more time to deploy the caller ID verification system because of the resources needed to transition to an IP network. This issue was discussed by industry stakeholders at FCC's July 2019 summit on the caller ID verification system. One industry stakeholder stated that when calls that begin on a traditional wireline network are uploaded to an IP network, the originating service provider on that IP network will sign the call with the lowest level of verification, and that that information, in combination with analytics, will help providers to know whether these calls can be trusted.
- **Verification of certain calls:** As of June 2019, ATIS and industry stakeholders were also working to determine how to ensure that calls from 911 operators or video relay service calls for deaf and hard of hearing users are not blocked if providers are unable to verify the caller is authorized to use the phone number.

[75]According to an ATIS representative, as of June 2019, the industry was discussing the possible creation of best practices regarding this issue.

FCC Has Actively Encouraged Deployment of the Caller ID Verification System and Been Engaged with Its Development

Since 2013, FCC has taken several steps to encourage the industry's caller ID verification initiative. In doing so, FCC's efforts have aligned with federal guidance for agency participation in private-sector standards activities to help address national priorities.[76] That guidance states that federal engagement in standards activities should aim to produce timely, effective standards that address legitimate regulatory, procurement, and policy objectives. The guidance also states that the federal government should assume an active role where necessary to ensure a rapid, coherent response to national challenges. Key steps FCC took to initiate and accelerate industry efforts—in line with the OMB guidance to produce timely and effective standards— are summarized below.[77]

- In March 2013, FCC's Chief Technology Officer presented a vision of developing a caller ID verification system to combat spoofing at an Internet Engineering Task Force meeting, later referred to as a "call to action" by a technology stakeholder who played a key role in developing this system.
- In July 2016, FCC's Chairman issued a call to action for providers to accelerate their efforts to develop this system. FCC also called for responses detailing provider efforts.

[76]Office of Science and Technology Policy, United States Trade Representative, Office of Management and Budget, *Memo on Principles for Federal Engagement in Standards Activities to Address National Priorities*, Memo M-12-08, (Washington, D.C.: Jan. 17, 2012). The memo provides that federal government engagement may be needed in limited policy areas where a national priority has been identified in statute, regulation, or administration policy. The memo followed a 1996 act that provides that federal agencies shall—when such participation is in the public interest and compatible with agency and departmental missions and authorities—participate with voluntary, private-sector, consensus-standards bodies in the development of technical standards. National Technology Transfer and Advancement Act of 1995, Pub. L. No. 104-113, § 12(d), 110 Stat. 775, 783 (1996). In addition, Office of Management and Budget's Circular A-119 encourages federal representatives to participate actively in standards development activities. See Office of Management and Budget, *Circular A-119: Federal Participation in the Development and Use of Voluntary Consensus Standards and in Conformity Assessment Activities*, (Washington, D.C.: Jan. 27, 2016).

[77]FTC has also played a role in encouraging industry to develop other ways to reduce the harmful effects of spoofing. For example, from 2012 to 2015, FTC staff sponsored four prize competitions to spur development of consumer products to block illegal robocalls.

- In December 2017, FCC directed one of its advisory bodies to, among other things, define criteria for selecting the system's governance authority and recommend milestones for system deployment. Consistent with the guidance that federal engagement should aim to produce timely, effective standards, FCC's Chairman urged service providers and standards groups to accelerate the development and deployment of these technical standards.
- In November 2018, the FCC Chairman sent letters to 14 U.S. providers and publicly demanded that that they adopt the caller ID verification system by the end of 2019.[78] While the demand did not legally require providers to deploy the system, the Chairman stated that if industry's progress lagged in 2019, FCC would take action to ensure widespread deployment. This demand and warning represent preliminary steps consistent with the guidance's call for the federal government to assume an active role where necessary to ensure a rapid, coherent response to national challenges.
- In June 2019, FCC issued a notice of proposed rulemaking that would require all providers to implement the technical system if major providers fail to do so by the end of 2019. The notice also requested comments on how FCC should determine whether it is necessary to mandate implementation of the technical system and how to evaluate whether major voice service providers have met the FCC's end of 2019 deadline for implementation.[79]

According to FCC officials and consistent with the federal guidance, FCC has engaged with ATIS, providers, and relevant technical stakeholders throughout their caller ID verification efforts. For example, FCC officials attended key meetings, and an FCC official submitted technical suggestions on standards development related to the caller ID verification system. ATIS representatives told us that FCC's engagement in these technical efforts was helpful, as FCC was able to ask questions and prompt those working on the standards to consider some of the broader

[78]The letters asked about each provider's plan to deploy the system. Thirteen of the 14 providers responded publicly with a time frame for deployment, while the 14th stated it was working towards the goal of implementing the system once the standards are finalized and approved. According to FCC officials, they selected the largest US providers and other providers whose networks might have unique characteristics that could affect system deployment. FCC officials added that, taken together, these providers serve the vast majority of U.S. consumers.

[79]34 FCC Rcd 4876 (2019).

issues that various stakeholders would be concerned about and needed to be addressed.

Furthermore, FCC is considering how, if at all, its role should evolve in the future. Notably, FCC's June 2019 notice also requested comments on what role FCC should have in the governance of the caller ID verification system, how to encourage carriers that maintain some portion of their network on legacy technology to implement elements of the system, and how FCC and industry can best leverage this system to combat illegal calls originating outside of the United States. FCC also directed staff to develop two reports over the next 2 years that, among other things, provide information on the state of deployment of this caller ID verification system. FCC officials stated that their efforts related to these issues encompass more than what is in the proposed regulations, as FCC will continue to monitor the work of the governance authority, the progress of service providers' implementation of the system, and industry's efforts to improve the effectiveness of the system and address remaining technical issues. Moreover, at FCC's July 2019 summit on the caller ID verification system, FCC's Chairman stated that FCC is prepared to issue rules in 2020 mandating that major providers implement the caller ID verification system if these major providers do not meet the 2019 deadline.

Agency Comments

We provided a draft of this report to FCC, FTC, and DOJ for review and comment. Each agency provided technical and editorial comments, which we incorporated as appropriate.

We are sending copies of this report to the appropriate congressional committees, the Chairman of the FCC, the Chairman of the FTC, the Attorney General, and other interested parties. In addition, the report is available at no charge on the GAO website at http://www.gao.gov.

If you or your staff any have questions about this report, please contact me at (202) 512-2834 or VonahA@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. GAO staff who made key contributions to this report are listed in appendix III.

Andrew Von Ah
Director, Physical Infrastructure Issues

Appendix I: List of Stakeholders GAO Interviewed

Table 2: List of Stakeholders GAO Interviewed

Category	Organization/individual interviewed
Call-blocking and analytics services	First Orion
	Hiya
	Nomorobo
	YouMail
Consumer groups	AARP
	Consumers Union
	National Consumer Law Center
Industry associations	CTIA – The Wireless Association
	NCTA - The Internet & Television Association
	NTCA - The Rural Broadband Association
	PACE - Professional Association for Customer Engagement
	U.S. Chamber of Commerce
	US Telecom – The Broadband Association
	VON Coalition – Voice on the Net Coalition
Knowledgeable stakeholders	Russ Housley - Internet Engineering Task Force
	Henning Schulzrinne - Former Federal Communications Commission Chief Technology Officer
	Richard Shockey - Session Initiation Protocol (SIP) Forum
Mobile phone manufacturer	Apple
Standards body	ATIS - The Alliance for Telecommunications Industry Solutions
Voice Service Providers	AT&T
	Google[a]
	US Cellular
	Verizon

Source: GAO interviews with stakeholders. | GAO-20-153.

[a]Google is also a mobile phone manufacturer.

Appendix II: Summary of Federal Agencies' Enforcement Actions Involving Telephone Calls that Allegedly Used Spoofed Caller ID

Table 3: Summary of Federal Agencies' Enforcement Actions Involving Telephone Calls that Allegedly Used Spoofed Caller ID, April 2006 to June 2019

Cases filed by	Defendant and date filed[a]	Summary of relevant alleged conduct	Description of judgment or proposed penalty, amount collected (if applicable), status as of August 2019[b]
The Federal Communications Commission	Security First of Alabama; Apr. 12, 2011	Security First of Alabama placed 43 robocalls to 33 consumers without either prior express consent or an established business relationship.	Civil penalty of $342,000; collected $0; closed
	Travel Club Marketing; Oct. 31, 2011	The parties placed at least 185 robocalls, all of which were unsolicited to over 142 consumers, who had not consented to the robocalls and the majority of whom had placed their telephone number on the National Do Not Call Registry (DNC Registry), which prohibits marketing calls to listed numbers.	Civil penalty of $2,960,000; in 2017, DOJ settled the case for $50,000; collected $970; closed
	Steven Blumenstock; Aug. 2, 2016	To assist a colleague with a harassment and stalking campaign, Blumenstock made threatening calls to the colleague's ex-wife by spoofing phone numbers familiar to the ex-wife, such as the numbers of her child's school and her parents' home.	Civil penalty of $25,000; collected $25,000; closed
	Best Insurance Contracts, Inc., and Philip Roesel; Aug. 4, 2017	Over a 3-month period, Roesel's company made over 21-million spoofed robocalls, which targeted elderly and low-income individuals to generate leads and sales of health insurance coverage. The call volume also disrupted an emergency medical-paging service.	Civil penalty of $82,106,000; collected $0; with Department of Justice for collection

	Adrian Abramovich; June 22, 2017	Over a 3-month period, Abramovich's company made over 96-million spoofed calls that appeared to come from well-known travel and hospitality companies promoting vacation deals. Consumers were then directed to a call center that sold vacations deals from lesser-known companies. The call volume also disrupted an emergency medical-paging service.	Civil penalty of $120,000,000; collected $0; with Department of Justice for collection
	Affordable Enterprises of Arizona, LLC; Sept. 26, 2018	Affordable Enterprises made spoofed calls to consumers to try to sell them home improvement and remodeling services. Many of the consumers had placed their numbers on the DNC Registry.	Proposed civil penalty of $37,525,000; open
The Federal Trade Commission	Mutual Consolidated Savings (MCS); June 25, 2009	Defendants telemarketed a "rapid debt reduction" program for a fee initiated by either a live representative or a robocall. Numerous calls used spoofed caller ID information and were placed to numbers on the DNC Registry as well as to consumers who had previously asked the company not to call them again. The program offered substantially lower credit card interest rates and promised full refund if the consumer did not save the promised amount. In many instances, the defendants did not obtain substantially lower interest rates and did not provide a refund.	Equitable monetary relief of $22,508,306; collected $1,500,000; closed
The Federal Trade Commission	Voice Touch, LLC; May 13, 2009	Defendants sold telemarketing services that delivered robocalls, often using spoofed caller ID information, to sell extended automobile warranties to consumers or inform the consumer of a recall without any information on the recipient's vehicle. If the consumer responded to the call, they were transferred to the defendant's call center that falsely represented that they were affiliated with the recipient's automobile dealership or manufacturer. Defendants also regularly called numbers on the DNC Registry as well as consumers who had previously asked defendants or their clients not to call them again.	Equitable monetary relief of $48,000,000; collected $3,130,147; closed
	Transcontinental Warranty, Inc.; May 13, 2009	Defendants or their telemarketing services initiated robocalls— regularly using spoofed caller ID information—to sell vehicle service contracts that they characterized as "extended automobile warranties" with no knowledge of the recipient's warranty and no affiliation with the recipient's auto dealership or manufacturer. Instead the warranty contracts were sold by an independent third party for $2,000 to $3,000. Defendants also regularly called numbers on the DNC Registry or consumers who had previously asked defendants not to call them again.	Equitable monetary relief of $24,000,000; collected $0; closed

	Economic Relief Technologies, LLC; Nov. 30, 2009	Defendants or their telemarketers initiated telemarketing robocalls, often using spoofed caller ID information, for credit card interest rate reduction services and charged a fee for worthless services or vehicle warranties, which consumers were falsely told were affiliated with their vehicle manufacturer. In numerous instances, defendants called numbers on the DNC Registry, as well as consumers who had previously asked defendants not to call them again.	Equitable monetary relief of $25,238,411; collected $0; closed
	2145183 Ontario, Inc.; Nov. 30, 2009	Defendants engaged in the similar alleged conduct as in *Economic Relief Technologies, LLC* for credit card interest rate reduction services.	Equitable monetary relief of $8,332,213; collected $300,000; closed
	JPM Accelerated Services, Inc.; Nov. 30, 2009	Defendants engaged in similar alleged conduct as in *Economic Relief Technologies, LLC* for credit card interest rate reduction services.	Equitable monetary relief of $5,935,680; collected $23,948; closed
	Nelson Gamble & Associates LLC, et al.; Sept. 10, 2012	Defendants or their telemarketing service initiated robocalls, in many instances using spoofed caller ID information, to sell worthless debt settlement services. In numerous instances, defendants falsely represented the services would be provided by attorneys. In numerous instances, defendants called numbers on the DNC Registry.	Equitable monetary relief of $4,638,915; collected $17,694; closed
The Federal Trade Commission	Pecon Software Ltd., et al.; Sept. 24, 2012	After using spoofed U.S. phone numbers, including from the recipients' local area and from a university, the India-based defendant, and affiliated defendants falsely led U.S. consumers to believe that their computers had viruses and other malware problems, and that defendants were from or affiliated with well know computer manufacturers and could provide technical support. Consumers, whose numbers were in numerous instances on the DNC Registry, spent up to $300 each for unnecessary computer security and technical support services.	Equitable monetary relief of $504,644; collected $0; closed
	The GreenSavers, LLC, et al.; Oct. 22, 2012	Defendants engaged in similar alleged conduct as in *Economic Relief Technologies, LLC* for credit card interest rate reduction services.	Equitable monetary relief of $3,879,114; collected $60,000; closed
	A+ Financial Center, et al.; Oct. 23, 2012	Defendants engaged in similar alleged conduct as in *Economic Relief Technologies, LLC* for credit card interest rate reduction services.	Equitable monetary relief of $9,238,155; collected $25,000; closed
	The Cuban Exchange, Inc.; Nov. 28, 2012	Defendants made robocalls and spoofed FTC's toll-free number as part of a scheme to obtain consumers' bank account information and other personal information. Defendants falsely claimed consumers would receive refund payments resulting from FTC lawsuits and directed consumers to enter their personal information in a website run by defendants.	Fines were not assessed
	ELH Consulting, LLC, et al.; Oct. 22, 2013	Defendants engaged in similar alleged conduct as in *Economic Relief Technologies, LLC* for credit card interest rate reduction services.	Equitable monetary relief of $12,099,852; collected $1,000,000; closed

	Worldwide Info Services, Inc., et al.; Jan. 6, 2014	Defendants and their telemarketers made unsolicited robocalls, sometimes using spoofed caller ID information, falsely advertising free medical alert systems to vulnerable consumers. Consumers were then directed to telemarketers and charged monthly service fees and had difficulty canceling the service, resulting in additional charges to their account.	Equitable monetary relief of $22,989,609; collected $79,000; closed
	Caribbean Cruise Line, Inc., et al.; Mar. 3, 2015	Caribbean Cruise Line LLC (CCL) made billions of political survey robocalls, using spoofed caller ID information, as part of an illegal telemarketing campaign to generate sales leads. Consumers were offered a free cruise for completing a survey, and if they opted-in, were transferred to a CCL telemarketer that charged fees for the cruise and additional travel packages. Several telephone companies supplied CCL with large quantities of phone numbers that CCL could change the names that appeared on consumers' caller ID.	Civil penalty of $15,125,000; collected $531,500; closed
	All Us Marketing LLC, et al.; June 29, 2015	Defendants engaged in similar alleged conduct as in *Economic Relief Technologies, LLC* for credit card interest rate reduction services.	Equitable monetary relief of $4,890,797; collected $50,600; closed
The Federal Trade Commission	Lifewatch Inc., et al.; June 30, 2015	Defendants and their telemarketers made unsolicited robocalls, sometimes with spoofed caller ID information, to falsely advertise free medical alert systems to vulnerable consumers. Consumers were then directed to telemarketers and charged fees for the monthly service, which consumers had difficulty canceling.	Equitable monetary relief of $25,266,886; collected $2,000,000; closed
	Aaron Michael Jones, et al.; Jan. 3, 2017	Defendants assisted their telemarketer clients by sending billions of robocalls, often with spoofed caller ID information to numbers on the DNC Registry, to generate sales leads. This telemarketing campaign resulted in more than 30,000 complaints to the FTC and its enforcement partners.	Civil penalty of $15,300,000; collected $513,000; closed
	ABC Hispana Inc., et al.; Feb. 13, 2017	Defendants and their Peruvian-based telemarketers made calls, often using spoofed caller ID information to sell English-language instructional materials and products to Spanish-speaking consumers throughout the U.S. Telemarketers impersonated government officials, help centers, well-known companies, or radio stations, and promoted false incentives that culminated in threats to consumers if products were not purchased. The defendants collected millions of dollars from consumers.	Equitable monetary relief of $6,315,023; collected $0; closed
	Jasjit Gotra, et al.; Mar. 22, 2018	Defendant and his home security service company were recidivist violators of the Telemarketing Sales Rule, violating a 2014 Stipulated Final Order. The company utilized third-parties to call consumers, at times using spoofed caller ID information, including neighbor caller IDs or calling numbers on the DNC Registry, to generate sales leads.	Civil penalty of $15,435,033; collected $300,000; open

	James Christiano, et al.; May 31, 2018	Defendant and his companies were involved with a large-scale telemarketing scheme. The telemarketers paid defendant to write software that sent autodialed calls, including robocalls, to consumers using spoofed caller ID information from an uploaded, unlimited list of caller ID numbers. 64-million neighbor spoofed calls were placed through his company, generating almost 8,000 consumer complaints to the FTC.	Civil penalty of $7,750,000; collected $1,400,000; closed
The Department of Justice on behalf of the Federal Trade Commission	Srikanth Venkataraman; Apr. 26, 2006	Defendants placed unwanted telemarketing calls, transmitting either spoofed or no caller ID information, to sell mortgage loans, refinancing, and other products and services to consumers whose numbers were on the DNC Registry. Consumers were unable to contact the telemarketer to stop the unwanted calls.	Civil penalty of $1,220,000; collected $45,000; closed
	Civic Development Group, LLC; Sept. 27, 2007	Defendants placed telemarketing calls to consumers, without transmitting caller ID information, or substituted the donor service telephone number, to solicit charitable contributions for police, firefighter and other non-profit organizations. The defendants misled consumers by telling them that defendants' telemarketers worked directly for the charities. The charities received a small percentage of the donations.	Civil penalty of $18,775,000; collected $18,775,000; closed
The Department of Justice on behalf of the Federal Trade Commission	Global Mortgage Funding, Inc.; Oct. 30, 2007	Defendant, a telemarketer, made hundreds of thousands of calls to consumers on the DNC Registry in an attempt to sell financial products. The defendant failed to transmit caller ID information.	Civil penalty of $6,000,000; collected $0; closed
	Guardian Communication, Inc.; Nov. 6, 2007	Defendant "blasted" phone numbers with pre-recorded telemarketing pitches, immediately terminating calls when a live consumer answered, leaving "dead air "and giving them no opportunity to ask to be placed on the company's entity-specific no-call list. Defendants also failed to transmit accurate caller ID information to consumers – instead transmitting the text "Cust Service," "Services, Inc.," "Card Services," "DWC," or "LTR" as the name of the caller	Civil penalty of $7,892,242; collected $150,000; closed
	Feature Films for Families, Inc.; May 5, 2011	Defendants initiated telemarketing calls to consumers, including those on the DNC Registry, to sell family friendly DVDs or theatre tickets and solicited donations for charities. Defendants also failed to transmit accurate caller ID information and, instead, provided names such as "CUSTOMER SVC," "FAMILY VALUE CB" or "VELVETEEN";	Civil penalty of $45,487,735; collected $487,735; closed
	Sonkei Communications, et al.; Nov. 17, 2011	Defendants sold telemarketing services, including robocalling, to telemarketers that offered credit card services, home security systems, and grant procurement programs. Defendants enabled their clients to transmit spoofed caller ID information, such as displaying "SERVICE MESSAGE" or "SERVICE ANNOUNCEMENT." The calls generated tens of thousands of complaints from consumers and businesses.	Civil penalty of $395,000; collected $0; closed

	Roy Cox, Inc., et al.; Dec. 12, 2011	Defendant and several domestic and international companies he controlled sold telemarketing services that delivered robocalls for clients selling credit card interest rate reduction programs, extended automobile warranties, and home security systems. Defendants also transmitted spoofed caller ID information, such as CARD SERVICES," "CREDIT SERVICES" or "PRIVATE OFFICE," to consumers with phone numbers on the DNC Registry or who had not provided their written consent for solicitation.	Civil penalty of $1,100,000; collected $0; closed
	Americall Group, Inc.; Dec. 15, 2011	Defendant provided telemarketing services for clients, including major banks and insurance and credit card companies. Defendant, in many cases, transmitted spoofed caller ID information, such as displaying "Gas Rebate Center."	Civil penalty of $500,000; collected $500,000; closed
	JGRD, Inc., et al.; Feb. 24, 2012	Defendants marketed its telemarketing services to clients, advertising that it could deliver prerecorded messages to more than one million potential customers a day. Defendants provided clients with the ability to control the caller ID information, including the displayed number and name, such as "CUSTOMERSVC," "CUST SERVICE," "SERVICE," "SERVICE ANNOUNC" and "INSURANCECO." The defendants also transmitted calls to consumers on the DNC Registry.	Civil penalty of $1,000,000; collected $10,000; closed
The Department of Justice on behalf of the Federal Trade Commission	KFJ Marketing, LLC, et al.; Mar. 10, 2016	As part of its campaign to generate leads for solar panel installation companies, defendant, a telemarketing service, made robocalls, including statements such as "this is an urgent message about your energy bills" and "Stop the 14 percent increase coming soon." Defendant initiated over 1.3 million calls to phone numbers on the DNC Registry, and in numerous instances, transmitted spoofed caller ID information.	Civil penalty of $1,400,000; collected $155,000; closed
	Derek J. Bartoli; June 21, 2019	Defendant developed and operated an autodialer, which blasted out large volumes of robocalls to consumers, who were then transferred to a live telemarketer selling products or services. Calls were placed to consumers listed on the DNC Registry and transmitted spoofed caller ID information.	Civil penalty of $2,141,043; collected $0; closed

The Department of Justice	Silvio Carrano, et al.; May 28, 2010	Carrano and three other defendants, with help from co-conspirators, advertised fraudulent business opportunities through the Internet and in newspapers, including distributorships for coffee, greeting cards, and vending machines, and included claims such as "Earn $50K - $250K year!" and "Coffee Dist. Guaranteed Accts … Unlimited Profit Potential." U.S. consumers were urged to call typically toll-free domestic numbers, which were then routed to Costa Rica. Defendants and their co-conspirators made false statements about the companies' locations, expected profits, the services the companies could provide, and the authenticity of the personal references for the distributorships. If potential investors called the domestic phone number provided for any of the references, the calls were again routed to Costa Rica to the defendants and co-conspirators. Most investors paid at least $10,000.	Carrano was sentenced to 97 months' imprisonment and 3 years' supervised release and ordered to pay over $9,000,000 in restitution.
	James O'Rourke, et al.; Nov. 23, 2011	James O'Rourke and two other defendants advertised business opportunities through the Internet and in newspapers. The advertisements promoted various distributorships, such as for coffee and vending machines and included claims such as "Earn $50K - $250K year!" Readers were typically urged to call toll-free numbers. Potential purchasers were given false references with domestic numbers that were routed to Costa Rica. Defendants made false statements about the companies' location and expected profits from the companies. Most purchasers paid at least $10,000.	O'Rourke was sentenced to 24 months' imprisonment and ordered to pay $6,412,006.19 in restitution. Total collected: $2,460.
	Sean Rosales; Nov. 29, 2011	Rosales, with help from co-conspirators, advertised business opportunities through the Internet and in newspapers. The advertisements promoted distributorships such as for coffee and vending machines and included claims such as "Earn $50K - $250K year!" Readers were typically urged to call toll free numbers. Potential purchasers were given false references with domestic numbers that were routed to Costa Rica. Defendant made false statements about the companies' location and expected profits from the companies. Most purchasers paid at least $10,000.	Rosales was sentenced to 97 months' imprisonment and ordered to pay $7,322,264.88 in restitution. Total collected: $9,856.46.
The Department of Justice	Onieke M. Barnett, et al.; Aug. 8, 2012	Barnett and another defendant, with help from co-conspirators, ran a lottery scheme in Jamaica and made calls that transmitted spoofed caller ID information, including U.S. area code numbers, to induce elderly victims in the U.S. to send money to cover fees for lottery winnings that they had not won. Defendants made calls from Jamaica utilizing VoIP technology that allowed them to use a telephone number with a U.S. area code.	Barnett was sentenced to 60 months' imprisonment and ordered to pay $94,456 in restitution. Total collected: $200.

Jeffrey R. Bonner, et al.; Jan. 17, 2013	Bonner and two other defendants based in Costa Rica, with help from co-conspirators, made calls to U.S. residents transmitting fake caller ID information and falsely informing them that they had won a sweepstakes and had to send money via Western Union for a "refundable insurance fee." The defendants, with help from co-conspirators, would often represent themselves as FTC or other government agency agents. To claim prizes, U.S. residents were provided telephone numbers with U.S. area codes, which were answered by the defendants at call centers in Costa Rica.	Bonner was sentenced to 180 months' imprisonment and 3 years' supervised release and ordered to pay $9,688,486.47 in restitution, to be paid jointly and severally with several defendants in related cases.
Daniel Carrasco and Fredrico Martin Gioja; July 25, 2013	Defendants used Spanish-language television commercials and cold calls from a call center in Argentina to Spanish-speaking U.S. consumers falsely stating that they were affiliated with Spanish-language television networks and offered consumers products, including English-language learning products, along with free gifts. Defendants sent consumers products they did not order and without gifts and sometimes charged them for packages consumers had not ordered. If consumers refused to accept the packages, consumers were at times threatened with arrest, deportation, and fines on their gas and electric bills.	Carrasco was sentenced to 121 months' imprisonment. Co-defendant Gioja was sentenced to 108 months' imprisonment. Forfeiture was obtained from both defendants, consisting of five pieces of real property, 11 bank accounts, one boat, one automobile, one motorcycle, and two firearms. No restitution was ordered.
Maria Haydee Luzula, et al.; Apr. 29, 2014	Defendant and a co-defendant's common enterprise obtained the names of Spanish-speaking U.S. residents who had previously purchased products from unaffiliated companies. Call center employees in Peru, contacted the victims, claiming that they were calling from a legal department, a private entity or a state or city. The victims were told that they had failed to accept delivery of and pay for products purchased from unaffiliated companies and were liable for substantial costs incurred by those companies. Victims were threatened with deportation, detention, negative credit reports, confiscation of property and community service requirements for which they could not take time off work. Many victims made payments.	Luzula was sentenced to 165 months' imprisonment and ordered to pay $212,545 in restitution. Total collected: $0. Cuya (Luzula's co-defendant) was sentenced to 210 months' imprisonment and ordered to pay $212,545 in restitution. Total collected: $0.
Dominic H. Smith; June 2, 2014	Defendant and co-conspirators engaged in a lottery scheme based in Jamaica by falsely informing elderly victims that they had won a large monetary prize and fraudulently inducing them to pay fees in advance of receiving their purported lottery winnings. Victims sent hundreds of thousands of dollars to Smith, who acted as a middleman, kept a portion of the money, and provided the rest to co-conspirators.	Sentenced to 27 months' imprisonment and 1 year of supervised release. Ordered to pay $724,408.79 in restitution.

The Department of Justice	Maurice A. Levy, et al.; Aug. 5, 2014	Defendants Maurice Levy and Derrick Levy, Jamaican citizens, owned and operated telemarketing call centers in Costa Rica engaged in sweepstakes schemes directed, at least in part, at victims residing in the U.S. Defendants called victims using VoIP, utilizing numbers with area codes that made it appear that they originated in the U.S. Defendants caused victims to send funds until these victims either ran out of money or realized they were being defrauded. Defendants are currently fugitives.	Court order administratively closed case as to Maurice Norman Levy, subject to reopening upon apprehension or appearance of defendant.
	Andrew Smith, et al.; Oct. 22. 2014	Defendants, with help from co-conspirators, made calls transmitting spoofed caller ID information to U.S. residents, falsely informing them that they had won money from a sweepstakes contest in excess of $350,000 and that they were required to send funds to Costa Rica to purchase insurance coverage for the delivery of their prizes, which would be fully refundable and returned along with their prize winnings. Individuals who sent payment were re-contacted and told that they had actually won the first prize of $3,500,000, requiring additional payment. The spoofed caller ID information displayed area codes that made it appear that the calls originated from within the U.S. rather than from Costa Rica.	Defendant Smith was sentenced to 25 years' imprisonment and 2 years' supervised release. Ordered to pay $10,222,838.76 in restitution jointly and severally with other co-conspirators and forfeit $406,324.96. Defendant Brissett was sentenced to 30 months' imprisonment. Defendant Harris was sentenced to 7 years' imprisonment and 2 years' supervised release, and ordered to forfeit $3,756,762.36. Defendant Griffen was sentenced to 20 years' imprisonment and 3 years' supervised release, and ordered to forfeit $182,439. Defendant Hernandez was sentenced to 5 years' imprisonment and 2 years' supervised release. Total collected: $1,910.
	Cesar Luis Kou Reyna; Aug. 27, 2015	Reyna, with help from co-conspirators, operated call centers in Peru and maintained shipping operations in Miami. Defendants placed cold calls to Spanish-speaking U.S. residents using VoIP technology to sell low quality cell phones and natural products. Defendants also sought to defraud and extort money from victims who were falsely told that they had failed to accept and pay for products they had never ordered. Defendants claimed during calls that they were lawyers, sometimes calling from a "legal department" of a state or city in the U.S. Numerous victims were coerced into making payments after receiving these calls.	Reyna was sentenced to 58 months' imprisonment and ordered to pay $522,043.05 in restitution. Total collected: $875.

	Dino Nastasi, et al.; Sept. 16, 2015	Nastasi and several other defendants owned, managed, and worked in one or more call centers in Costa Rica. Defendants, with help from co-conspirators, engaged in sweepstakes schemes, directed at, at least in part, victims residing in the U.S. Nastasi, 12 other defendants, and unnamed co-conspirators falsely represented themselves as being agents of the FTC, the "Department of Consumer Affairs," or another U.S. government agency, and used VoIP telephone lines utilizing numbers with area codes associated with Washington, D.C., making it appear the calls originated from the U.S.	Nastasi was sentenced to 102 months' imprisonment followed by 3 years' supervised release and ordered to pay $11,236,857.65 in restitution jointly and severally with all co-defendants.
The Department of Justice	Frank M. Schiavone and Lewis Ricker; Dec. 15, 2015	Schiavone and Ricker, with help from co-conspirators, worked in at least one telemarketing call center in Costa Rica in a sweepstakes scheme. Like other sweepstake schemes, Schiavone induced victims to make payments in order to receive fictional sweepstakes winnings.	Schiavone was sentenced to 48 months' imprisonment and 3 years' supervised release and was ordered to pay $399,852.86 in restitution jointly and severally. Ricker was sentenced to 52 months' imprisonment and 3 years' supervised release. Total collected: $1,187.
	Ryan J. Vallee; Mar. 16, 2016	Defendant remotely hacked into the social media, email and online shopping accounts of almost a dozen minor females and threatened to delete, deface and make purchases from their accounts unless the victims sent sexually explicit photographs of themselves. Defendant obtained sexually explicit photographs of the girls and their friends and distributed them to others. Communications were sent to his victims using a text message spoofing or anonymizing service.	Sentenced to 96 months' imprisonment.
	Richard Antonucci, et al.; May 20, 2016	Antonucci worked in at least one telemarketing call center in Costa Rica. He would call victims and falsely inform them that they had won a sweepstakes and had to send money to Costa Rica to pay various fees, and taxes. He also falsely induced victims who had made the initial payment into making additional payments via Western Union wire services by making new misrepresentations (e.g. the prize amount had increased due to clerical error).	Antonucci was sentenced to 57 months imprisonment and 3 years' supervised release and was ordered to pay $624,145.88 in restitution.

	Braulio de La Cruz Vasquez, et al.; July 14, 2016	Defendants, with help from co-conspirators, participated in a global cell phone scheme that involved compromising cellphone customers' accounts and "cloning" their phones to make fraudulent international calls through defendant's call center. As a result, defendant received tens of thousands of dollars from at least one VoIP company for routing international calls through his call center.	Defendant Vasquez was sentenced to 65 months' imprisonment and 2 years' supervised release. Restitution ordered reserved. Defendant Batista was sentenced to 51 months' imprisonment and 3 years' supervised release and ordered to pay $794,418 in restitution. Defendant Calderon was sentenced to 3 years' imprisonment and 3 years' supervised release and ordered to pay $170,000 in restitution. Defendant Santana was ordered to pay $170,000 in restitution. Total collected: $425.
	Ronald J. Mendleski; Sept. 28. 2016	Defendant provided leads to clients who operated fraudulent telemarketing companies in Costa Rica, Jamaica, and other foreign countries known by defendant to be centers of telemarketing fraud. Clients sent the defendant scripts to be used in the calls that on their face were fraudulent schemes. In some instances the telemarketer claimed that the victim had won vast sums of money in a sweepstakes that the victim had never entered and occasionally the telemarketer posed as a representative of a government entity or legitimate private business.	Sentenced to 48 months' imprisonment and 3 years' supervised release. Ordered to pay $92,000 in restitution.
The Department of Justice	Sunny M. Joshi, et al.; Oct. 19, 2016	Joshi and co-defendants, with help from co-conspirators, acted in a complex scheme in which individuals from call centers located in, India, called U.S. residents and impersonated officials from the I.R.S. and U.S. Citizenship and Immigrations Services or loan officers for pay day loans. Defendants used "spoofed" telephone numbers to make calls appear to originate from a U.S. federal agency, and threatened victims with arrest, imprisonment, fines or deportation for immigration or tax violations unless the fines were paid immediately. Victims who agreed to pay were instructed to purchase general purchase reloadable cards or wire money.	Twenty-four defendants in the U.S. have pleaded guilty. Sixty-one defendants have been charged. Joshi pleaded guilty to one count of conspiracy to commit money laundering, was sentenced to 151 months' imprisonment and 3 years' supervised release, and was ordered to pay $8,970,396.15 in restitution joint and severally with co-defendants. Ordered to forfeit $5,398,467.98. Total collected: $23,269.46. Co-defendants were ordered to pay varying amounts of restitution and forfeiture, and sentences ranged from 3 years' probation to 20 years' imprisonment and 3 years' supervised release. Additional property in preliminary order of forfeiture (value to be determined): 25 gold bars, 6 silver bars, 2 silver coins, iPhone 5, iPhone 7, out-of-circulation U.S. currency, iTunes gift card.

	Robert L. Stencil, et al.; Apr. 19, 2017	Stencil founded a company incorporated in NV and operating in Charlotte, NC. Stencil, in a scheme that included eight other defendants and additional co-conspirators, contacted targeted individuals by telephone and internet to induce victims to purchase the company's stock. In the contacts, the defendants and co-conspirators made false representations to investors regarding things such as the nature of the company's facilities, operations, management, expertise, achievements, and stock value. Defendants used the proceeds of the stock sales for their personal benefit. One defendant, along with co-conspirators working in his call center in Costa Rica, used VoIP to call victims, allowing them to use recognizable U.S. area codes to make it appear that their calls were made from the U.S.	Stencil was found guilty. Not yet sentenced. Ordered to pay $1,149,253.75 in restitution jointly and severally with two other defendants. The remaining defendants were ordered to pay $1,949,034.17 in restitution jointly and severally. Two defendants were sentenced to 5 months' imprisonment and 2 years' supervised release each. Two more defendants were sentenced to 3 years' probation each. Total collected: $31,525.
	William P. Nanry; Oct. 3, 2017	Defendant sold fake "leads"— misrepresenting that the names, phone numbers, and addresses he provided were for individuals who had consented to telemarketing pitches— to a small group of telemarketing clients. Many of these leads were used by fraudulent telemarketers, and some individuals were victimized by the fraudulent telemarketers	Not yet sentenced
	Michael D. Kent; Oct. 10, 2017	Kent, with help from co-conspirators, targeted victims who owned interests in timeshare properties to obtain fraudulent fees for faked sales of their timeshares. Defendant would contact the victim and introduce them to a co–conspirator who posed as a "buyer," who used false name, address, phone number, and email address, and agreed to buy the property. The defendant would then contact the victim and inform them they needed to send between $500 to $1,500 to cover costs, such as closing costs or transfer fees to complete the sale. Victims paid over $550,000.	Kent was sentenced to 63 months' imprisonment and 3 years' supervised release and ordered to pay $557,542.50 in restitution.
The Department of Justice	Okigbo, et al.; Feb. 9, 2018	Okigbo, four other defendants, and unnamed co-conspirators engaged in a scheme that defrauded victims in the U.S. and other countries of over $7 million by fraudulently offering investment funding or to facilitate the transfer of a supposed inheritance in exchange for paying certain advance fees. Okigbo would disperse victims' funds into various bank accounts upon receiving them. Other defendants or co-conspirators impersonated U.S. bank representatives—at in-person meetings, over the Internet, and over the phone, using spoofed numbers that made it appear the calls originated from the state where the U.S. bank was headquartered, to convince victims to send money.	Defendants were not yet sentenced.

Lee Elbaz; Mar. 22, 2018	Defendant was an employee of a company that provided retention services (services to obtain additional deposits from investors) through the use of communications by email and phone to individuals in the U.S. and elsewhere. Representatives falsely claimed they were located in London U.K. including use of phone numbers with area codes associated with the U.K. This case involved sale of certain option contracts which were not traded on a legal and regulated contract market in the U.S. The Defendant and co-conspirators obtained the maximum account deposit from investors and then took steps to ensure that investors lost the money in their accounts. Defendants and others received commissions based on net investor deposits not investor profits.	Elbaz was not yet sentenced.
Ryan S. Lin; Apr. 9, 2018	Defendant engaged in extensive cyberstalking activity targeting Jane Doe 1 and associates. During the same time, defendant engaged in a separate cyberstalking activity, including sending unsolicited illicit images and over 120 hoax bomb threats, aimed at other victims unassociated with Jane Doe 1. The defendant used a number of techniques to mask his identity online, including accessing the internet using a service that anonymizes IP addresses ("TOR" for "The Onion Router"); using Virtual Private Network ("VPN") services; using anonymous overseas texting services; and using encrypted email providers that do not respond to U.S. law enforcement and/or do not maintain IP logs or other records. Many messages were sent from a text messaging service where a user can select a different number and then send text messages, as well as photographs, that appeared to originate from any selected spoofed number.	Sentenced to 210 months' imprisonment and 60 months' supervised release. Ordered to pay $12,802.85 in restitution to Jane Doe 1.
Joel Edwin Kurzynski; Aug. 23, 2018	Defendant conducted cyberstalking and threat campaigns, including numerous spam phone calls.to multiple Washington state residents. The campaigns involved death threats, body shaming, and hate speech, amongst other activities.	Sentenced to 30 months' imprisonment and 3 years' supervised release. Ordered to pay $37,682.99 in restitution.

Source: GAO analysis of Federal Communications Commission, Federal Trade Commission, and Department of Justice legal documents and other information provided by the agencies. | GAO-20-153

Note: According to officials at the Department of Justice, Federal Communications Commission, or Federal Trade Commission, each of these cases involved spoofing or blocking of caller-ID information, regardless of whether we mention spoofing in the column showing relevant elements of alleged conduct. We selectively mention spoofing in this column to provide additional context for some of these cases.

[a]Date of Notice of Apparent Liability (NAL), Final Order, or Indictment.

[b]In many of the cases filed by the Federal Trade Commission or filed by the Department of Justice on behalf of the Federal Trade Commission, defendants were also banned from engaging in future telemarketing efforts. The table does not include information on these bans. In addition, Federal Trade Commission officials said that in many of the cases filed by the Federal Trade Commission or filed by the Department of Justice on behalf of the Federal Trade Commission, the judgements were partially suspended based on the defendants' ability to pay as the Commission determined by a defendant's net worth and assets. Further, the officials said that if the defendant misrepresents his or her financial position, the entire judgment can become due under a clause that is part of the judgement.

Appendix III: GAO Contact and Staff Acknowledgments

GAO Contact:

Andrew Von Ah, (202) 512-2834 or VonahA@gao.gov.

Staff Acknowledgments:

In addition to the individual named above, other key contributors to this report were Alwynne Wilbur, Assistant Director; David Goldstein, Analyst-in-Charge; Mark Canter; Joshua Cicala; Jennifer Clayborne; Kristen Farole; Jeffery Haywood; Gina Hoover; Delwen Jones; Jenna Lada; Hannah Laufe; Harold Podell; Cheryl Peterson; and Malika Rice.

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through our website. Each weekday afternoon, GAO posts on its website newly released reports, testimony, and correspondence. You can also subscribe to GAO's email updates to receive notification of newly posted products.

Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's website, https://www.gao.gov/ordering.htm.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

Connect with GAO

Connect with GAO on Facebook, Flickr, Twitter, and YouTube.
Subscribe to our RSS Feeds or Email Updates. Listen to our Podcasts.
Visit GAO on the web at https://www.gao.gov.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact FraudNet:

Website: https://www.gao.gov/fraudnet/fraudnet.htm

Automated answering system: (800) 424-5454 or (202) 512-7700

Congressional Relations

Orice Williams Brown, Managing Director, WilliamsO@gao.gov, (202) 512-4400,
U.S. Government Accountability Office, 441 G Street NW, Room 7125,
Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, DC 20548

Strategic Planning and External Liaison

James-Christian Blockwood, Managing Director, spel@gao.gov, (202) 512-4707
U.S. Government Accountability Office, 441 G Street NW, Room 7814,
Washington, DC 20548