

Telephone Robocall Abuse Criminal Enforcement and Deterrence Act

2020 Report to Congress



EXECUTIVE SUMMARY

The Telephone Robocall Abuse Criminal Enforcement and Deterrence Act (“the TRACED Act”) (Public Law 116-105) directs the Attorney General, in consultation with the Chairman of the Federal Communications Commission, to convene an interagency working group (“the Working Group”) to study prosecutions under section 227(b) of the Communications Act of 1934 (47 U.S.C § 227(b)). The TRACED Act directs the Working Group to provide a report to Congress including (a) any recommendations regarding the prevention and prosecution of such violations and (b) a description of what progress, if any, relevant Federal departments and agencies have made in implementing those recommendations.

This 2020 report reflects that the past nine months have seen considerable progress in law enforcement activity and collaboration by Working Group members, undertaken to halt the scourge of unlawful robocalls plaguing the American public. As described below, these efforts have educated Working Group members about the origin and transmission of unlawful robocalls, and they have allowed participating federal and state agencies to develop strategies for successfully disrupting and litigating against perpetrators and facilitators of illegal robocall activity.

THE WORKING GROUP

After enactment of the TRACED Act, the Attorney General, through the Consumer Protection Branch of the Department of Justice's Civil Division, convened the Working Group. Membership includes representatives of the Consumer Financial Protection Bureau, the Department of Justice, the Federal Bureau of Investigation, the Federal Communications Commission, the Federal Trade Commission, Homeland Security Investigations, the National Association of Attorneys General, the Social Security Administration Office of Inspector General, the Postal Inspection Service, and the Treasury Inspector General for Tax Administration. Members of the Working Group are in frequent contact with one another and held full Working Group meetings in March, May, and July of 2020. The Working Group's objectives included studying the requirements of the TRACED Act, improving coordination among agencies and with the private sector, and promoting the identification, investigation, deterrence, and prosecution of criminal robocall schemes. The present report has been prepared by the Department of Justice in consultation and coordination with the other Working Group members.

A. Working Group Strategies – Development and Implementation

1. Filed Enforcement Actions

A number of Working Group members have initiated enforcement actions against individuals and entities involved in perpetrating and/or facilitating massive unlawful robocall campaigns against the American public. Through these cases and related investigations, Working Group members have uncovered the current *modus operandi* of criminal robocall schemes and the networks that allow them to flourish. The Working Group's efforts in these

cases have been critical to law enforcement's and regulatory agencies' development of strategies for combatting criminal robocall schemes.

U.S. Department of Justice

In January 2020, the Department of Justice (Department) brought two civil actions against U.S.-based Voice over Internet Protocol (VoIP) companies and their owners, alleging that the defendants knowingly transmitting fraudulent robocalls to U.S. consumers.¹ The cases were investigated by a multi-agency coalition of Working Group members, including the Social Security Administration's Office of the Inspector General, the Postal Inspection Service, and the Treasury Inspector General for Tax Administration.

The complaints alleged that the defendants engaged in wire fraud schemes by knowingly serving as "gateway carriers" for fraudulent calls; that is, the defendants received fraudulent robocalls from foreign customers and relayed those calls into the U.S. telecommunications system. The Department alleged that defendants in both cases were warned numerous times that they were transmitting fraudulent robocalls, including calls impersonating the Social Security Administration, yet the defendants continued to carry those calls and facilitate foreign-based fraud schemes targeting Americans. Many of the schemes perpetrated through these robocalls consisted of fraudulent marketing campaigns directed at elderly and vulnerable victims. The Department's filings in the cases contain detailed discussions of the telecommunications industry practices that allow fraudulent robocalls to pass from foreign call centers to U.S. victims.

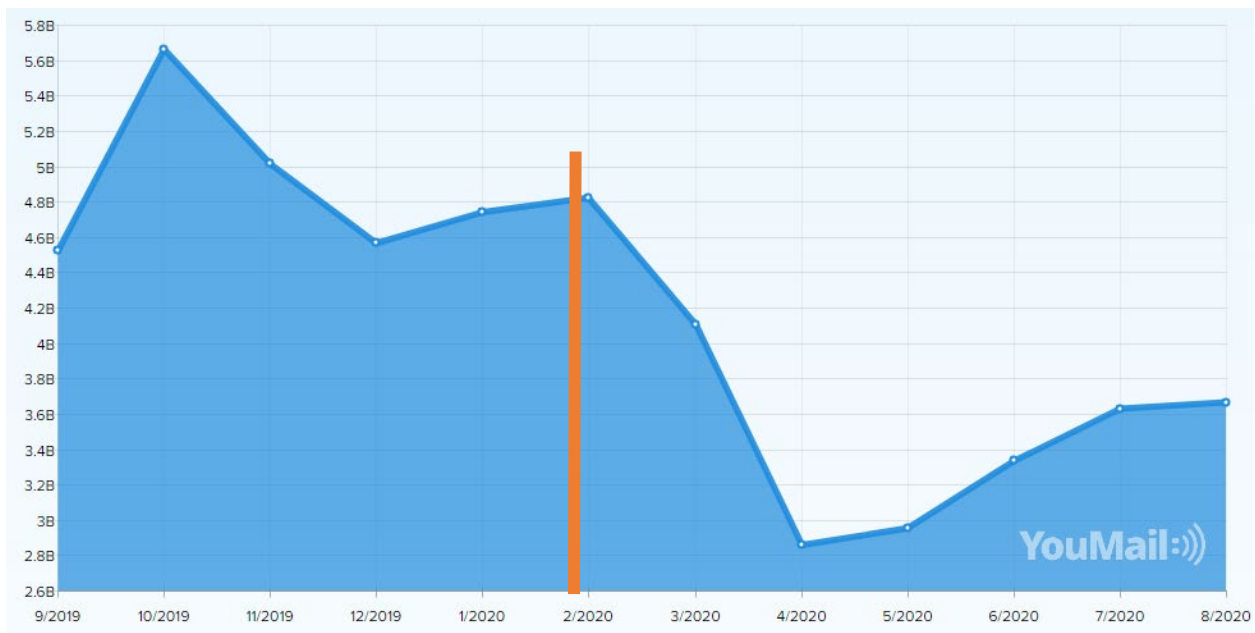
¹ Press Release, U.S. Dept. of Justice, *The Department of Justice Files Actions to Stop Telecom Carriers Who Facilitated Hundreds of Millions of Fraudulent Robocalls to American Consumers* (Jan. 28, 2020), <https://www.justice.gov/opa/pr/departments-justice-files-actions-stop-telecom-carriers-who-facilitated-hundreds-millions>.

In both cases, the reviewing federal courts issued both preliminary and permanent injunctions against the defendants, prohibiting them from, among other things, carrying VoIP calls destined for U.S. consumers and selling U.S. phone numbers.² In one of the cases, for instance, the U.S. District Court for the Eastern District of New York issued an order and opinion granting the government’s request to enjoin the defendants’ conduct and making factual findings about the defendants’ services as gateway providers. The court stated: “Over time, it became increasingly clear that [defendants] knew or should have known the complaints [they received] evidenced a widespread pattern of fraudulent calls being transmitted over their network.” The court further found “probable cause to conclude that the defendants are engaged in a widespread pattern of telecommunications fraud, intended to deprive call recipients in the Eastern District of New York and elsewhere of money and property.”

In the months following the Department’s action in these cases, the number of robocalls that reached U.S. consumers were hundreds of millions of robocalls fewer per month than in the preceding months. The below graph from YouMail,³ a software developer that monitors automated call patterns and behaviors and sells proprietary robocall blocking software, shows the decline in transmitted robocalls immediately after the Department filed its complaints:

² Press Release, U.S. Dept. of Justice, *District Court Enters Permanent Injunction Shutting Down Telecom Carriers Who Facilitated Hundreds of Millions of Fraudulent Robocalls to Consumers in The United States* (Aug. 26, 2020), <https://www.justice.gov/opa/pr/district-court-enters-permanent-injunction-shutting-down-telecom-carriers-who-facilitated>.

³ Robocall Index, <https://robocallindex.com/> (last visited Oct. 8, 2020).



Federal Trade Commission

Illegal robocalls remain a significant consumer protection problem and one of consumers’ top complaints to the Federal Trade Commission (FTC). Through the first nine months of Fiscal Year 2020, the FTC received more than 2.7 million complaints about unwanted calls, including 1.9 million complaints about robocalls. The FTC is using all of the tools at its disposal to fight these illegal calls and has brought 149 enforcement actions against 505 corporations and 402 individuals since the National Do Not Call Registry began accepting registrations in 2003.⁴

The FTC recently concluded its first action against VoIP service provider Globex.⁵ The FTC alleged in December 2019 that the VoIP company provided marketers with the means to

⁴ See FTC Robocall Initiatives, www.consumer.ftc.gov/features/feature-0025-robocalls. In its enforcement actions, the Commission has collected over \$160 million in equitable monetary relief and civil penalties. See Enforcement of the Do Not Call Registry, www.ftc.gov/news-events/media-resources/do-not-call-registry/enforcement.

⁵ The FTC amended its complaint in the *Educare Centre Services* fraud litigation to add Globex Telecom, Inc. *FTC v. Educare Centre Services, Inc.*, No. 3:19-cv-196 (W.D. Tex., Am. Compl. filed Dec. 3, 2019), www.ftc.gov/enforcement/cases-proceedings/192-3033/educare-centre-services-inc.

make the alleged illegal calls. The settlement requires Globex and its U.S.-based subsidiaries to pay \$1.95 million and to abide by client screening and monitoring provisions.⁶ Since December 2019, the FTC has seen a sharp drop in the number of robocall complaints, although there were likely many factors accounting for this drop—including more aggressive blocking by phone companies and warning letters from the FTC and others—.⁷

Last year, the FTC coordinated “Operation Call It Quits,” a law enforcement crackdown that included 94 total actions by the FTC and 25 federal, state, and local agencies.⁸ Collectively, the defendants in these cases were responsible for making more than a billion illegal robocalls to consumers. Other FTC cases reflect the FTC’s enforcement efforts against illegal telemarketing. For example, in *Grand Bahama Cruise Line*, the FTC is litigating claims against defendants who allegedly made or facilitated millions of illegal calls to consumers pitching free cruise vacations.⁹ In *Career Education Corporation*, the operator of several post-secondary schools agreed to pay \$30 million to settle FTC charges that it used sales leads from lead generators that

⁶ Press Release, F.T.C., *Globex Telecom and Associates Will Pay \$2.1 Million, Settling FTC’s First Consumer Protection Case Against a VoIP Service Provider* (Sept. 22, 2020), www.ftc.gov/news-events/press-releases/2020/09/globex-telecom-associates-will-pay-21-million-settling-ftcs-first. Among other things, under the monitoring requirements, Globex and its subsidiaries will be required to block any calls made by their clients that appear to come from certain suspicious phone numbers, including emergency numbers like 911, unassigned or invalid numbers, or international numbers that would charge consumers a large amount should they attempt to dial it. They will also be required to block calls that use spoofing technology, and to terminate their relationship with any telemarketer or other high-risk client that receives three or more USTelecom Traceback Requests (an official industry complaint about unlawful calls) or line carrier complaints in a 60-day period.

⁷ Press Release, F.T.C., *Court Halts Operations of VoIP Service Provider after the FTC and Ohio Alleged that It Helped Promote Credit Card Interest Reduction Scheme* (Dec. 5, 2019), www.ftc.gov/news-events/press-releases/2019/12/court-halts-operations-voip-service-provider-after-ftc-ohio; FTC Blog Post, *The FTC keeps attacking robocalls* (Apr. 3, 2020), <https://www.consumer.ftc.gov/blog/2020/04/ftc-keeps-attacking-robocalls>; FTC Blog Post, *Robocall reports still down, FTC still fighting* (June 15, 2020), www.consumer.ftc.gov/blog/2020/06/robocall-reports-still-down-ftc-still-fighting.

⁸ Press Release, F.T.C., *FTC, Law Enforcement Partners Announce New Crackdown on Illegal Robocalls* (June 25, 2019), www.ftc.gov/news-events/press-releases/2019/06/ftc-law-enforcement-partners-announce-new-crackdown-illegal.

⁹ *FTC v. Grand Bahama Cruise Line, LLC*, No. 6:20-cv-52 (M.D. Fla. filed Jan. 10, 2020), www.ftc.gov/enforcement/cases-proceedings/162-3005/grand-bahama-cruise-line-llc.

called consumers on the National Do Not Call Registry, making false representations that the callers were affiliated with the U.S. military.¹⁰

The FTC also continues to engage with industry stakeholders and to support industry initiatives to authenticate caller ID numbers and curb illegal calling. For example, since January 2020, the FTC has sent 15 warning letters to VoIP service providers and others that may have been assisting and facilitating the transmission of robocalls using coronavirus-related messages (six of the most recent letters were sent jointly with the Federal Communications Commission).¹¹ To identify these entities, the FTC used information provided by the USTelecom Industry Traceback Group, a collaborative effort of companies across the wireline, wireless, VoIP, and cable industries that actively trace and identify the source of illegal robocalls.¹² The FTC also regularly works with its state, federal, and international partners to combat illegal robocalls.¹³

¹⁰ *FTC v. Career Education Corp.*, No. 1:19-cv-5739 (N.D. Ill. filed Aug. 27, 2019), www.ftc.gov/enforcement/cases-proceedings/152-3264/career-education-corporation. There are many other recent cases in which the FTC has stopped illegal robocalls. *See, e.g., U.S. v. Derek Jason Bartoli*, No. 6:19-cv- 01160 (M.D. Fla. filed June 21, 2019), www.ftc.gov/enforcement/cases-proceedings/182-3105/derek-jason-bartoli (banning a robodialer responsible for more than 57 million calls to numbers on the Do Not Call Registry in just six months in 2017); *U.S. v. Media Mix 365*, No. 8:19-cv-01243 (C.D. Cal. filed June 21, 2019), www.ftc.gov/enforcement/cases-proceedings/182-3070/media-mix-365-llc (obtaining \$264,000 in civil penalties from a solar panel lead generator and its owners who called millions of numbers on the National Do Not Call Registry); *FTC v. First Choice Horizon LLC*, No. 6:19-cv-1028 (M.D. Fla. filed June 3, 2019), www.ftc.gov/enforcement/cases-proceedings/172-3161-x190029/first-choice-horizon-llc (shutting down illegal robocalls allegedly used to contact financially distressed consumers with offers of bogus credit card interest rate reduction services). The FTC's case against fraudulent business opportunity 8 Figure Dream Lifestyle, described above, was also part of Operation Call it Quits. *See FTC v. 8 Figure Dream Lifestyle LLC*, No. 8:19-cv- 01165 (C.D. Cal. filed June 12, 2019), www.ftc.gov/enforcement/cases-proceedings/182-3117/8-figure-dream-lifestyle-llc.

¹¹ Press Release, F.T.C., *FTC and FCC Send Joint Letters to VoIP Service Providers Warning against 'Routing and Transmitting' Illegal Coronavirus-related Robocalls* (Apr. 3, 2020), www.ftc.gov/news-events/press-releases/2020/04/ftc-fcc-send-joint-letters-voip-service-providers-warning-against; Press Release, F.T.C., *FTC and FCC Send Joint Letters to Additional VoIP Providers Warning against 'Routing and Transmitting' Illegal Coronavirus-related Robocalls* (May 20, 2020), www.ftc.gov/news-events/press-releases/2020/05/ftc-fcc-send-joint-letters-additional-voip-providers-warning.

¹² *FTC Coronavirus Warning Letters to Companies*, www.ftc.gov/coronavirus/enforcement/warning-letters. On July 27, 2020, the FCC's Enforcement Bureau designated the USTelecom Industry Traceback Group as the official consortium for coordinating industry-led efforts to trace back the origin of suspected unlawful robocalls. <http://www.fcc.gov/document/fcc-designates-robocall-traceback-manager>.

¹³ *See, e.g.,* Press Release, F.T.C., *FTC and FCC to Host Joint Policy Forum on Illegal Robocalls* (Mar. 22, 2018), www.ftc.gov/news-events/press-releases/2018/03/ftc-fcc-host-joint-policy-forum-illegal-robocalls; Press Release, F.T.C., *FTC and FCC Seek Exhibitors for an Expo Featuring Technologies to Block Illegal Robocalls* (Mar. 7,

Federal Communications Commission

1. Enforcement Actions Under the TRACED Act

The Federal Communications Commission (FCC) has prosecuted illegal spoofing activities, and continues to do so. Since enactment of the TRACED Act, the FCC initiated the largest enforcement action in FCC history against the worst campaign of unlawful robocalls and spoofing ever investigated by the FCC. In June 2020, the FCC issued a Notice of Apparent Liability proposing a forfeiture of \$225,000,000 against persons allegedly responsible for making approximately one billion spoofed robocalls in the first quarter of 2019 alone. These calls transmitted prerecorded messages falsely claiming affiliation with major health insurance providers in the United States.¹⁴ If sustained at a Forfeiture Order proceeding, the proposed fine would be the largest in FCC history.¹⁵

In addition, the FCC continues to pursue other illegal spoofing activities. For example, in January 2020, the FCC issued a Notice of Apparent Liability and proposed a fine of nearly \$13

2018), www.ftc.gov/news-events/press-releases/2018/03/ftc-fcc-seek-exhibitors-expo-featuring-technologies-block-illegal; see also Memorandum of Understanding Among Public Authorities of the Unsolicited Communications Enforcement Network Pertaining to Unlawful Telecommunications and SPAM (May 2016), www.ftc.gov/policy/cooperation-agreements/international-unlawful-telecommunications-spam-enforcement-cooperation; Press Release, F.T.C., *FTC Signs Memorandum of Understanding With Canadian Agency To Strengthen Cooperation on Do Not Call, Spam Enforcement* (Mar. 24, 2016), www.ftc.gov/news-events/press-releases/2016/03/ftc-signs-memorandum-understanding-canadian-agency-strengthen. The FTC also held a workshop in January 2020 titled “You Don’t Say: An FTC Workshop on Voice Cloning Technologies” that examined the use of cloned voices to perpetuate telemarketing fraud. See FTC Workshop, *You Don’t Say: An FTC Workshop on Voice Cloning Technologies* (Jan. 28, 2020), www.ftc.gov/news-events/events-calendar/you-dont-say-ftc-workshop-voice-cloning-technologies.

¹⁴ John C. Spiller; Jakob A. Mears; Rising Eagle Capital Group LLC, et al., Notice of Apparent Liability for Forfeiture, FCC 20-74 (June 10, 2020).

¹⁵ Press Release, F.C.C., *FCC Proposes Record \$225 Million Fine for Massive Spoofed Robocall Campaign Selling Health Insurance* (Jun. 9, 2020), <https://docs.fcc.gov/public/attachments/DOC-364824A1.pdf>.

million against Scott Rhodes for apparently making a series of particularly disruptive spoofed robocalls.¹⁶

2. Warning Letters Regarding Illegal Coronavirus Calls

Working Group members have collaborated with one another and with responsible industry participants to warn voice service providers identified as facilitating unlawful robocall traffic. These warnings set forth the harm they cause and the law enforcement consequences of continuing to assist unlawful schemes.

The onset of the Novel Coronavirus (COVID-19) outbreak greatly increased the importance of this collaboration, as illegal calls bombarded consumers with bogus coronavirus-related claims. As a result, the FCC, the FTC, and the Department of Justice began working closely together in March 2020 to identify fraudulent robocalling campaigns that exploited the evolving health crisis. As an outcome of this collaboration, the FTC and FCC took rapid action to disrupt campaigns by sending warning letters to gateway providers; that is, voice service providers that received the illegal calling campaigns from foreign customers and relayed them into the U.S. telecommunications network.

On April 3, 2020, and again on May 20, 2020, the FCC and the FTC jointly sent warning letters to a total of five gateway providers and one originating provider; the letters demanded that the recipient providers cease carrying fraudulent COVID-19-related robocall traffic immediately.¹⁷ The letters warned the providers that if they failed to terminate the offending

¹⁶ See *Scott Rhodes a.k.a. Scott David Rhodes, Scott D. Rhodes, Scott Platek, Scott P. Platek, Notice of Apparent Liability for Forfeiture*, 35 FCC Rcd 882 (2020).

¹⁷ See Press Release, F.C.C., *FCC, FTC Demand Gateway Providers Cut Off Robocallers Perpetrating Coronavirus-Related Scams from United States Telephone Network* (Apr. 3, 2020), <https://www.fcc.gov/document/fcc-ftc-demand-gateway-providers-cut-covid-19-robocall-scammers>; Press Release,

calls within 48 hours, the FCC would authorize domestic phone companies to block all traffic from their networks. Within 48 hours of the issuance of each letter, FCC received responses from each of the six providers to confirm that the offending robocall traffic had been terminated. These claims were verified by traceback experts at USTelecom.¹⁸

3. FCC Rulemakings Following Enactment of the TRACED Act

a. Blocking of Illegal Robocalls

The FCC has taken several regulatory steps to encourage the blocking of illegal robocalls since the passage of the TRACED Act. On July 16, 2020, the FCC adopted rules to encourage phone companies to block illegal and unwanted robocalls before they reach consumers.¹⁹ The

F.C.C., *FCC, FTC Demand Robocall-Enabling Service Providers Cut Off Scammers* (May 20, 2020), <https://www.fcc.gov/document/fcc-ftc-demand-robocall-enabling-service-providers-cut-scammers>. See also Letter from Rosemary C. Harold, Chief, Enforcement Bureau, Federal Communications Commission & Lois C. Greisman, Associate Director, Division of Marketing Practices, Federal Trade Commission, to Chris Cordero & Scott Kettle, Connexum (Apr. 3, 2020) (available at <https://docs.fcc.gov/public/attachments/DOC-363522A3.pdf>) (Connexum Letter); Letter from Rosemary C. Harold, Chief, Enforcement Bureau, Federal Communications Commission & Lois C. Greisman, Associate Director, Division of Marketing Practices, Federal Trade Commission, to Barry Augustinsky, SIPJoin Holdings Corp. (Apr. 3, 2020) (available at <https://docs.fcc.gov/public/attachments/DOC-363522A4.pdf>) (SIPJoin Letter); Letter from Rosemary C. Harold, Chief, Enforcement Bureau, Federal Communications Commission & Lois C. Greisman, Associate Director, Division of Marketing Practices, Federal Trade Commission, to Muhammad U. Khan, VoIP Terminators dba BLMarketing (Apr. 3, 2020) (available at <https://docs.fcc.gov/public/attachments/DOC-363522A5.pdf>) (BLMarketing Letter); Letter from Rosemary C. Harold, Chief, Enforcement Bureau, Federal Communications Commission & Lois C. Greisman, Associate Director, Division of Marketing Practices, Federal Trade Commission, to Franklin Fawzi, CEO, Inetelepeer Cloud Communications LLC (May 20, 2020) (available at <https://docs.fcc.gov/public/attachments/DOC-364482A3.pdf>) (Inetelepeer Letter); Letter from Rosemary C. Harold, Chief, Enforcement Bureau, Federal Communications Commission & Lois C. Greisman, Associate Director, Division of Marketing Practices, Federal Trade Commission, to Craig Densen, CEO, PTGi International Carrier Services, Inc. (May 20, 2020) (available at <https://docs.fcc.gov/public/attachments/DOC-364482A4.pdf>) (PTGi Letter); Letter from Rosemary C. Harold, Chief, Enforcement Bureau, Federal Communications Commission & Lois C. Greisman, Associate Director, Division of Marketing Practices, Federal Trade Commission, to Vitaly Potapov, CEO, RSCom LTD (May 20, 2020) (available at <https://docs.fcc.gov/public/attachments/DOC-364482A5.pdf>) (RSCom Letter)

¹⁸ The FCC and FTC also sent letters to USTelecom thanking the Industry Traceback Group for its assistance in identifying the robocalls. See Press Release, F.C.C., *FCC, FTC Demand Gateway Providers Cut Off Robocallers Perpetrating Coronavirus-Related Scams from United States Telephone Network* (Apr. 3, 2020), <https://www.fcc.gov/document/fcc-ftc-demand-gateway-providers-cut-covid-19-robocall-scammers>; News Release, FCC, *FTC Demand Robocall-Enabling Service Providers Cut Off Scammers* (May 20, 2020), <https://www.fcc.gov/document/fcc-ftc-demand-robocall-enabling-service-providers-cut-scammers>.

¹⁹ *Advanced Methods to Target and Eliminate Unlawful Robocalls*, CG Docket No. 17-59, Third Report and Order, Order on Reconsideration, and Fourth Further Notice of Proposed Rulemaking, 35 FCC Rcd 7614 (2020).

rules offer companies two safe harbors from liability for the unintended or inadvertent blocking of wanted calls, thus eliminating a concern that kept some companies from implementing robust robocall blocking efforts. The first safe harbor protects from liability voice service providers that use reasonable analytics, including caller ID authentication information, to identify and block illegal or unwanted calls.²⁰ The second safe harbor protects providers that block call traffic from bad-actor upstream voice service providers that pass illegal or unwanted calls along to other providers, when those upstream providers have been notified but fail to take action to stop these calls or fail to take affirmative steps to prevent new and renewing customers from originating illegal traffic.²¹ These safe harbors are meant to provide further assurance to phone companies and allow them to strengthen their efforts in the battle against illegal and unwanted robocalls. The rules also adopted certain protections for callers when calls are blocked in error.²²

In the same rulemaking, the FCC sought comment on several related issues, including further implementation of the TRACED Act's blocking-related provisions and requiring voice service providers to meet certain affirmative obligations.²³ Specifically, it sought comment on further expansion of the call blocking safe harbors, including a safe harbor for certain blocking at the network level.²⁴ Additionally, it sought comment on enhanced transparency and redress for both consumers and callers, including requiring timely notification to callers when calls are blocked and provision of a blocked calls list to consumers.²⁵ Finally, it proposed to require voice service providers to: (1) respond to traceback requests from the FCC, law enforcement, or the USTelecom Industry Traceback Group; (2) take effective steps to mitigate unlawful call traffic

²⁰ *Id.* at 7625-27, paras. 25-34.

²¹ *Id.* at 7627-31, paras. 35-45.

²² *Id.* at 7633-36, paras. 51-59.

²³ *Id.* at 7640-48, paras. 80-112.

²⁴ *Id.* at 7641-42, 7646 paras. 81-87, 104-106.

²⁵ *Id.* at 7643-44, 7646-48, paras. 91-94, 107-112.

when notified of that traffic by the FCC; and (3) take affirmative, effective measures to prevent new and renewing customers from using their networks to originate illegal calls.²⁶

In a separate proceeding, the FCC proposed actions to stop the robocall-related “one-ring” scam, as required by section 12 of the TRACED Act.²⁷ In this scam, consumers in the United States receive a call from a foreign country. After one ring, the scammer hangs up, causing the consumer to call back and incur significant phone charges (of which the scammer gets a share). The FCC sought comment on how it can implement the TRACED Act and build upon its efforts to combat the one-ring scam by promoting consumer education and outreach, coordinating with regulatory partners, and working more closely with industry to protect all Americans. It also sought comment on a proposed rule allowing voice service providers to block a voice call when such call purports to originate from a number that is highly likely to be associated with a one-ring scam.

b. STIR/SHAKEN Framework

One tool to combat illegal caller ID spoofing is caller ID authentication, which allows voice service providers to verify that the caller ID information transmitted with a particular call matches the caller’s number, which in turn helps to determine whether the call should be blocked or labeled.²⁸ One method of caller ID authentication is the STIR/SHAKEN framework, which was developed for internet protocol networks by industry technologists to authenticate caller ID

²⁶ *Id.* at 7644-46, paras. 95-103.

²⁷ *Protecting Consumers from One-Ring Scams*, CG Docket No. 20-93, Notice of Proposed Rulemaking, 35 FCC Rcd 4908 (2020).

²⁸ FCC, *Combatting Spoofed Robocalls with Caller ID Authentication*, <https://www.fcc.gov/call-authentication> (last visited June 9, 2020).

in order to determine if a call is spoofed.²⁹ Section 4 of the TRACED Act directs the FCC to require voice service providers to “implement the STIR/SHAKEN authentication framework” in the Internet Protocol (IP) portions of their networks, and “take reasonable measures to implement an effective call authentication framework” in the non-IP portions of their networks no later than June 30, 2021.³⁰

In March 2020, the FCC adopted a Report and Order and Further Notice of Proposed Rulemaking that requires all originating and terminating voice service providers to implement the STIR/SHAKEN framework in the IP portions of their networks by June 30, 2021.³¹ The FCC also offered proposals and sought comment on further efforts to promote caller ID authentication and implement section 4 of the TRACED Act, and on implementing section 6(a) of the TRACED Act, which concerns access to numbering resources.³² Many large voice service providers have already started implementing STIR/SHAKEN.³³

On September 30, the FCC will consider a Second Report and Order completing implementation of the caller ID authentication provisions of the TRACED Act. The Report and Order, if adopted, would (1) require voice service providers to either upgrade their non-IP networks to IP and implement STIR/SHAKEN, or work to develop a non-IP caller ID authentication solution; (2) establish extensions of the June 30, 2021, caller ID authentication implementation deadline for certain categories of providers, including small voice service

²⁹ *2019 Call Blocking Declaratory Ruling*, 34 FCC Rcd at 4883, para. 21. SHAKEN, or Signature-based Handling of Asserted information using toKENS, and STIR, or Secure Telephony Identity Revisited, uses public key cryptography to provide assurances that certain information about the transmitted caller ID is accurate. *Id.*

³⁰ TRACED Act, § 4(b)(1)(A), (B). In addition, the TRACED Act provides that “[t]he Commission shall prohibit providers of voice service from adding any additional line-item charges to consumer or small business customer subscribers for the effective call authentication technology required.” TRACED Act, § 4(b)(6).

³¹ *STIR/SHAKEN Order*, 35 FCC Rcd at 3252-68, paras. 24-56.

³² *Id.* at 3268-96, paras. 57-130.

³³ See, e.g., AT&T, *AT&T Activates Call Validation Displays*, (Dec. 18, 2019), https://about.att.com/story/2019/call_validation_displays.html; Verizon, *Helping our Customers Block Robocalls*, <https://www.verizon.com/about/responsibility/robocalls> (last visited June 9, 2020); T-Mobile, *Mobile Security*, <https://www.t-mobile.com/customers/mobile-security> (last visited June 9, 2020).

providers; (3) require voice service providers subject to an extension to implement a robocall mitigation program in the non-STIR/SHAKEN-enabled portions of their networks; (4) require all voice service providers to file a certification in a FCC database showing how they are acting to stem the origination of illegal robocalls; (5) establish a process by which providers that make early progress on caller ID authentication implementation can obtain an exemption from the June 30, 2021 deadline; (6) prohibit voice service providers from adding any line item charges to the bills of consumer or small business customer subscribers for caller ID authentication technology; and (7) require intermediate providers to implement the STIR/SHAKEN caller ID authentication framework in the IP portions of their networks by June 30, 2021.

c. Selecting a Private Consortium to Conduct Tracebacks

On March 27, 2020, the FCC adopted rules to create a process for selecting a single consortium that will conduct private-led efforts to trace back the origin of suspected unlawful robocalls. The registered consortium, among other responsibilities, will provide the FCC with a list of voice service providers that “received a request from the registered consortium to participate in private-led efforts to trace back the origin of suspected unlawful robocalls and refused to participate.” The USTelecom Industry Traceback Group was selected on July 27, 2020 to serve as the initial registered consortium.

State Actions

State Attorneys General are generally authorized to investigate unlawful telemarketing practices and unfair or deceptive trade practices pursuant to their respective state statutes, which allow civil, and in some cases, criminal, enforcement actions seeking penalties, damages, restitution, injunctions, and other appropriate relief. State Attorneys General also have authority to enforce the federal Telemarketing Sales Rule (“TSR”), 16 CFR 310, *et seq.* The Attorney

General for the State of Ohio, for example, worked with the FTC in filing their joint case against Globex Telecom, Inc., discussed above, for TSR violations.

State Attorneys General can also enforce the Telephone Consumer Protection Act (“TCPA”) and the FCC’s regulations promulgated pursuant to the TCPA, which restrict calls made with automatic telephone dialing systems or that feature prerecorded or artificially-voiced messages, prohibit calls to numbers on the National Do Not Call Registry, and prohibit some caller ID spoofing. In June 2020, the States of Arkansas, Indiana, Michigan, Missouri, North Carolina, North Dakota, Ohio, and Texas filed a complaint against Rising Eagle Capital Group LLC, JSquared Telecom LLC, John C. Spiller, II, and Jakob A. Mears, in U.S. District Court in the Southern District of Texas.³⁴ The case was a result of an investigative partnership with the FCC, which issued a Notice of Apparent Liability on the same day that the States’ action was filed in federal court.³⁵ The States’ complaint alleges that Defendants violated the federal TCPA and various state consumer protection laws by initiating billions of outbound telephone calls that deliver artificial or prerecorded voice messages to residential and/or cellular telephone numbers of residents in the Plaintiff States without the prior express consent of the called parties. The lawsuit alleges that Defendants bombarded consumers with robocalls offering extended car warranties and health care services and illegally engaged in caller ID spoofing in an effort to mislead and defraud victims. They are also accused of targeting phone numbers on the National Do Not Call Registry.

State Attorneys General have long collaborated with federal partners on tracking down illegal robocallers and violators of telemarketing laws. The National Association of Attorneys

³⁴ *Arkansas v. Rising Eagle Capital Group LLC*, No. 4:20-cv-02021 (S.D. Tex. 2020).

³⁵ See footnote 13, above.

General hosts a monthly call among State Attorneys General and numerous federal agencies to discuss Do-Not-Call investigations and developments. These federal agencies include DOJ, the FTC, the FCC, the Internal Revenue Service, and the Social Security Administration Office of Inspector General. More recently, State Attorneys General also formed the Robocall Technologies Working Group, a multistate coalition to investigate the technological solutions that voice service providers were developing and implementing to cut off illegal robocalls at their source.

Since the passing of the TRACED Act, State Attorneys General have worked closely with the USTelecom Industry Traceback Group. In accordance with the TRACED Act, state agencies recognize that tracing a call to its source requires immense state and federal collaboration and cooperation across the telecommunications industry, since a single call often passes through the networks of multiple voice service providers before reaching its final destination. Not only do traceback investigations identify entities and individuals conducting illegal robocalling campaigns, they also shed light on members of the telecommunications ecosystem that are assisting these illegal robocallers. The USTelecom Industry Traceback Group regularly provides State Attorneys General with the results of its traceback investigations, thereby helping law enforcement identify illegal robocallers and voice service providers who facilitate those calls.

B. The Working Group's Future

In addition to the above strategies, Working Group members are using decades of experience and creative thinking to develop new approaches to preventing unlawful robocalls. Some of these ideas involve work with private industry to more quickly and easily identify and cut off unlawful traffic. Others involve collaboration with foreign law enforcement that may

have a greater ability to quickly shut down call centers from which illegal robocalls emanate. Many of the originators of scam robocalls are located overseas; law enforcement, in partnership with the Department of Justice, are committed to taking all necessary steps to increase cooperation and collaboration with law enforcement partners overseas to end these crimes. The Working Group will use all available, lawful tools and relationships to prevent and deter their continuation, especially given that elderly Americans and other vulnerable groups are disproportionately affected by the fraud schemes perpetrated through robocalls.

In sum, the Working Group has worked hard to implement both the language and spirit of the TRACED Act, is committed to finding both short term and long term solutions, and welcomes the support and the continued commitment of Congress in the fight against unlawful robocall schemes.