Calendar No. 94

116TH CONGRESS *1st Session*	SENATE	REPORT 116–41

TELEPHONE ROBOCALL ABUSE CRIMINAL ENFORCEMENT AND DETERRENCE ACT

R E P O R T

OF THE

COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION

ON

S. 151

MAY 21, 2019.—Ordered to be printed

U.S. GOVERNMENT PUBLISHING OFFICE

89–010 WASHINGTON : 2019

SENATE COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION

ONE HUNDRED SIXTEENTH CONGRESS

FIRST SESSION

ROGER F. WICKER, Mississippi, *Chairman*

JOHN THUNE, South Dakota
ROY BLUNT, Missouri
TED CRUZ, Texas
DEB FISCHER, Nebraska
JERRY MORAN, Kansas
DAN SULLIVAN, Alaska
CORY GARDNER, Colorado
MARSHA BLACKBURN, Tennessee
SHELLEY MOORE CAPITO, West Virginia
MIKE LEE, Utah
RON JOHNSON, Wisconsin
TODD C. YOUNG, Indiana
RICK SCOTT, Florida

MARIA CANTWELL, Washington
AMY KLOBUCHAR, Minnesota
RICHARD BLUMENTHAL, Connecticut
BRIAN SCHATZ, Hawaii
EDWARD J. MARKEY, Massachusetts
TOM UDALL, New Mexico
GARY C. PETERS, Michigan
TAMMY BALDWIN, Wisconsin
TAMMY DUCKWORTH, Illinois
JON TESTER, Montana
KYRSTEN SINEMA, Arizona
JACKY ROSEN, Nevada

JOHN KEAST, *Staff Director*
DAVID STRICKLAND, *Minority Staff Director*

Calendar No. 94

116TH CONGRESS *1st Session* | SENATE | REPORT 116–41

TELEPHONE ROBOCALL ABUSE CRIMINAL ENFORCEMENT AND DETERRENCE ACT

MAY 21, 2019.—Ordered to be printed

Mr. THUNE, from the Committee on Commerce, Science, and Transportation, submitted the following

R E P O R T

[To accompany S. 151]

[Including cost estimate of the Congressional Budget Office]

The Committee on Commerce, Science, and Transportation, to which was referred (S. 151) to deter criminal robocall violations and improve enforcement of section 227(b) of the Communications Act of 1934, and for other purposes, having considered the same, reports favorably thereon with an amendment (in the nature of a substitute) and recommends that the bill, as amended, do pass.

PURPOSE OF THE BILL

The purpose of S. 151, the Telephone Robocall Abuse Criminal Enforcement and Deterrence (TRACED) Act, is to aid the American public by helping to reduce illegal and unwanted robocalls by improving the ability of the Federal Communications Commission (FCC or Commission) and law enforcement to impose additional penalties for intentional violations of the Telephone Consumer Protection Act (TCPA). The bill also improves adoption of technical solutions for blocking illegal robocalls, and convenes a Federal interagency working group to combat the dramatic rise in such calls.

BACKGROUND AND NEEDS

Unsolicited robocalls are among the top consumer complaints to the FCC, the Federal Trade Commission (FTC), and many State at-

torneys general.[1] Although the FCC and FTC are tasked with fighting these calls,[2] available data indicate that robocalls are likely to increase and continue to be a major concern for consumers.[3] A large number of these illegal robocalls are spoofed calls, which are typically scams.[4] It is estimated that in 2019, nearly 50 percent of all calls to mobile phones will be scam robocalls.[5] Another report estimates that robocalls rang Americans' phones almost 5 billion times in April 2019—that is close to 2,000 calls per second.[6] Furthermore, this growing trend of unwanted robocalls extends to ringless voicemail (also known as direct to voicemail calls).[7] Recent court decisions have found such messages to be subject to TCPA.[8] Illegal and abusive robocalls are a clear problem.

Consumers today are increasingly plagued by illegal robotic or prerecorded messages. Certain prerecorded messages are restricted under section 227, unless they fall within one of the established exceptions such as consent or an emergency purpose. The legislation provides the Commission flexibility to adopt rules and take enforcement action to combat unlawful calls and texts, whether they use existing technologies or technologies that may emerge in the future. The legislation is designed to provide an agile tool that can be used to combat robocalling abuses as technologies and methodologies of transmitting these pernicious calls evolve.

But not all robocalls are illegal or unwanted. The majority of companies who use robocalls are legitimate companies.[9] And valid robocalls can benefit consumers. Many important services are car-

---

[1] *See* Tony Romm, "Robo-callers rang Americans' phones 26 billion times last year. Now, Congress is taking aim." *The Washington Post*, April 2, 2019 (*https://www.washingtonpost.com/technology/2019/04/02/robo-callers-rang-americans-phones-billion-times-last-year-now-congress-is-taking-aim/?utm_term=.1b634c1c65bb*); Bill Moak, "Stop calling! Unwanted robocalls reaching epidemic proportions. States getting involved." *The Clarion Ledger*, March 11, 2019 (*https://www.clarionledger.com/story/news/2019/03/11/robocalls-ftc-mississippi-cracking-down/3090094002/*); Andy Rosen, "Congress is taking new steps to stop robocall scammers," *The Boston Globe*, November 26, 2018, (*https://www.bostonglobe.com/business/2018/11/25/congress-make-take-new-steps-stop-robocall-scammers/8Ca0oLNAbHOooDoQo6soII/story.html*); Tara Siegel Bernard, "Yes, It's Bad. Robocalls, and Their Scams, Are Surging." *The New York Times*, May 6, 2018 (*https://www.nytimes.com/2018/05/06/your-money/robocalls-rise-illegal.html*); "Illegal Robocalls: Calling All to Stop the Scourge," hearing before the Subcommittee on Communications, Technology, Innovation, and the Internet of the Senate Committee on Commerce, Science, and Transportation, 116th Congress (2019) (testimony of Hon. Doug Peterson, Attorney General of Nebraska) (*https://www.commerce.senate.gov/public/_cache/files/e57e0488-3705-44d5-8e45-63bd7043cd25/910F8B485BD5D8CE241D28BA1DEAF7AA.04-11-19peterson-testimony.pdf*) (Peterson testimony); *see also* Report on Robocalls, CG Docket No. 17–59, Federal Communications Commission (February 2019) (FCC Report) (*https://docs.fcc.gov/public/attachments/DOC-356196A1.pdf*).

[2] *See, e.g.*, the Telephone Consumer Protection Act, 47 U.S.C. 227 (TCPA); Do Not Call Implementation Act, 15 U.S.C. 6101.

[3] FCC report at 4–6 ("Youmail shows the estimated national volume of robocalls increasing from 29,082,325,500 in 2016 to 30,507,422,900 in 2017, and to 47,839,232,200 in 2018.").

[4] Susan Tompor, "Social Security calling? Nope, it's scammers out to grab your cash," *The Seattle Times*, December 15, 2018 (*https://www.seattletimes.com/business/social-security-calling-nope-its-scammers-out-to-grab-your-cash/*).

[5] Press release, First Orion, "Nearly 50% of U.S. Mobile Traffic Will Be Scam Calls by 2019" (September 12, 2018) (*https://firstorion.com/nearly-50-of-u-s-mobile-traffic-will-be-scam-calls-by-2019/*).

[6] April 2019 Nationwide Robocall Data, YouMail (*https://robocallindex.com/*).

[7] *See* Josh Saul, "Can Annoying Robocall Voicemails Be Stopped? Attorneys General, Angry Phone Owners Argue Against New Marketing Tactic," *Newsweek*, June 5, 2017 (*https://www.newsweek.com/voiceless-messages-robocall-fight-attorneys-general-fcc-comments-621055*).

[8] *See, e.g.*, *Saunders* v. *Dyck O'Neal, Inc.,* 319 F. Supp. 3d 907 (W.D. Mich. 2018) (concluding ringless voicemails are subject to the TCPA at the motion for summary judgement phase); *see also Schaevitz* v. *Braman Hyundai, Inc.*, Case No. 1:17–cv–23890–KMM, 2019 U.S. Dist. LEXIS 48906 (S.D. Fl. March 25, 2019) (holding that ringless voicemail is subject to TCPA as a matter of law.).

[9] Patricia Moloney Figliola, "Protecting Consumers and Businesses from Fraudulent Robocalls," Congressional Research Service (December 21, 2018) (*https://www.crs.gov/reports/pdf/R45070).*

ried out via robocalls when institutions and call recipients have established a prior relationship: pharmacies provide updates to consumers that a prescription is ready for pick up; school closing announcements provide families with important and timely information; banks provide customers with fraud alerts, data security breaches, and even calls to convey measures consumers may take to prevent identity theft following a breach;[10] auto manufacturers can warn vehicle owners of urgent safety recalls. These legitimate calls can have life or death consequences for the intended recipient. But, as the FCC has noted, "[t]he same characteristics that make [legitimate] robocalls appealing to businesses also make them appealing to scammers. Those seeking to defraud consumers can do so efficiently and cost-effectively using robocalls, maximizing their ill-gotten gains."[11] Unwanted or illegal robocalls threaten this critical communication when frustrated recipients, fearing unwanted or illegal robocalls, are hesitant to answer their phones.[12]

Illegal robocallers often pose as legitimate businesses or government entities to trick individuals. For example, callers can fake their Caller ID to suggest the call originates from the Internal Revenue Service, a bank, or a local utility.[13] Often these calls threaten that some form of legal or financial jeopardy will result if the recipient does not follow instructions.[14] Faking or falsifying the Caller ID is known as "spoofing." A number is "spoofed" when the Caller ID information is manipulated or altered to display anything other than the originating telephone number.[15] "Spoofing" is illegal if done "with the intent to defraud, cause harm, or wrongfully obtain anything of value."[16] In some instances, "spoofing" is used legitimately to protect the caller or show affiliation with a specific entity. For example, a battered women's shelter might disguise its telephone number to protect the shelter's true number, which could be tracked and used to locate the center. A doctor calling patients from her cellphone may "spoof" her office number to help her patients know who is calling and to avoid giving out personal contact information.[17] But, despite these examples, as technology has progressed, it has allowed malicious and illegal robocallers to dramatically increase their ability to target consumers.

On June 22, 2017, the FCC issued a Notice of Apparent Liability (NAL) for Forfeiture finding an individual, Adrian Abramovich, apparently liable for perpetrating one of the largest spoofed robocall

---

[10] "Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991," Declaratory Ruling and Order, 30 FCC Rcd. 7961 (2015).

[11] FCC report at 4.

[12] Tara Siegel Bernard, "Yes, It's Bad. Robocalls, and Their Scams, Are Surging," *The New York Times*, May 6, 2018 (*https://www.nytimes.com/2018/05/06/your-money/robocalls-rise-illegal.html*) (noting that a surgeon failed to respond to a phone call from an emergency room believing it to be a robocall, which caused the surgeon to lose valuable time in responding to the injured individual).

[13] FCC report at 4.

[14] Michelle Singletary, "Robocalls have these retirees afraid to answer their phones," *The Washington Post*, March 8, 2019 (*https://www.washingtonpost.com/business/2019/03/08/tech-support-scams-other-schemes-are-hitting-seniors-hard-costing-millions/?noredirect=on&utm_term=.bd10b4d8d833*).

[15] *See* "Rules and Regulations Implementing the Truth in Caller ID Act of 2009," Report and Order, 26 FCC Rcd 9114, 9115, para. 1 (2011) (stating that spoofing may also involve manipulating or altering the caller ID to display a name or other text (i.e., anything other than the originating number).

[16] Truth in Caller ID Act, 15 U.S.C. 227(e).

[17] Sarah Krouse, "Stop Robocalling Me!"; "I Didn't!", *The Wall Street Journal*, January 1, 2019 (*https://www.wsj.com/articles/stop-robocalling-me-i-didnt-11546261200*).

campaigns that the FCC had ever investigated.[18] The NAL asserted that Mr. Abramovich was responsible for nearly 100 million illegal robocalls during a 3-month period, which equals over 1 million calls each day and nearly 44,000 such calls each hour.[19] These calls used spoofed numbers, appearing on a recipient's Caller ID to originate from a local number, increasing the odds that the recipient would find the number familiar or trustworthy. The robocalls would offer vacations and cruises to Mexico, the Caribbean, and Florida, and would falsely claim affiliation with well-known American travel and hospitality companies, including TripAdvisor, Expedia, Marriott, and Hilton. But trusting recipients would actually be connected to one of several unaffiliated travel agencies that had contracted with Mr. Abramovich to receive calls generated by his network. These travel agencies worked with Mexico-based call centers engaged in selling timeshares and vacation packages to Mexican timeshare facilities.

In the NAL, the FCC proposed a fine of $120 million against Mr. Abramovich for apparently violating the Truth in Caller ID Act of 2009.[20] The FCC also cited—but did not fine—Mr. Abramovich for the separate and additional offenses of making illegal robocalls in violation of the TCPA.[21] The FCC may not impose fines on those it does not regulate, like Mr. Abramovich, for violations of the Communications Act or FCC rules until a subsequent violation after a citation has been issued.[22] As Senator John Thune noted in a recent hearing, requiring the FCC to issue a warning citation before it can act against illegal robocallers and the current 1-year statute of limitations are hampering Federal enforcers from holding bad actors accountable.[23] Moreover, the citation requirement allows malicious robocallers to simply set up shop under a different corporate name and continue their malfeasance.

On October 10, 2017, then-Commerce Committee Chairman Thune sent a letter to Mr. Abramovich inquiring about his involvement with a number of companies that have allegedly made millions of robocalls. On April 18, 2018, the Senate Committee on Commerce, Science, and Transportation held a hearing on abusive robocalls, with Mr. Abramovich appearing before the Committee pursuant to a subpoena.[24] He spoke to the availability of software that allows illegal robocallers to make thousands of automated calls with the click of a button. Mr. Abramovich's testimony and responses highlight that the current policies in place are an ineffective deterrent for individuals violating the law.[25]

---

[18] Adrian Abramovich, Marketing Strategy Leaders, Inc., and Marketing Leaders, Inc., Notice of Apparent Liability for Forfeiture, FCC 17–80, June 22, 2017 (*https://docs.fcc.gov/public/attachments/FCC-17-80A1.pdf*) (NAL).

[19] NAL.

[20] NAL.

[21] Adrian Abramovich, Marketing Strategy Leaders, Inc., and Marketing Leaders, Inc., Citation and Order, DA 17–593, June 22, 2017 (*https://docs.fcc.gov/public/attachments/DA-17-593A1.pdf*).

[22] *See* 47 U.S.C. 503(b)(5); *see also* 47 CFR 1.80(a)(5).

[23] "Illegal Robocalls: Calling All to Stop the Scourge," hearing before the Subcommittee on Communications, Technology, Innovation, and the Internet of the Senate Committee on Commerce, Science, and Transportation, 116th Congress (2019) (statement of Sen. John Thune, Chairman, Subcommittee on Communications, Technology, Innovation, and the Internet) (Thune comments).

[24] "Abusive Robocalls and How We Can Stop Them," hearing before the Senate Committee on Commerce, Science, and Transportation, 115th Congress (2018) (*https://www.commerce.senate.gov/public/index.cfm/hearings?ID=E0EB17D2-A895-40B4-B385-F94EA2716957*).

[25] Id.

To combat illegal robocalls, stronger penalties are needed. At the recent Senate Subcommittee on Communications, Technology, Innovation, and the Internet hearing, "Illegal Robocalls: Calling All to Stop the Scourge," witnesses testified on the need for stronger enforcement mechanisms and the ability for law enforcement to bring criminal enforcement.[26] As Senator Thune noted, robocallers view the risk of getting caught and paying civil fines as a cost of business.[27] Nebraska Attorney General Doug Peterson acknowledged just that, stating that, "a lot of these violators probably perceive it that way, as if they're fine to move on. I think when you bring up criminal penalties that's when you get their attention."[28] Another witness responded, "[I]ndividuals like that [recidivist robocaller] definitely need to be targeted through criminal enforcement. The best way to prevent illegal robocalls is to stop them from ever being made and the best way to ensure that is to put the people that are making them behind bars."[29]

In addition to stronger enforcement and enhanced civil and criminal penalties, it is necessary to implement call authentication technologies to reduce robocalls. As robocallers often block or spoof Caller ID, the call recipient does not know the true caller. STIR/SHAKEN, an industry-developed call-authentication protocol, provides a standards-based means for an originating provider to assert a calling number's legitimacy, and provides a means for terminating providers to verify that the assertion itself is legitimate and trace the call back to its network entry point. Although some in the voice services industry have begun implementing this technology, the TRACED Act would help to ensure the speedy implementation of these authentication technologies and protect consumers. The TRACED Act would direct the FCC to require implementation of the STIR/SHAKEN authentication framework in the Internet protocol networks of those voice service providers who do not implement the technologies on their own.

According to the FCC, it faces several enforcement challenges in investigating illegitimate robocalls. First, many illegal robocallers are based in foreign countries.[30] And although Congress has provided the FCC with jurisdiction over foreign caller ID spoofers,[31] the FCC needs cooperation from foreign governments to effectively enforce anti-robocall regulations. Thus, the Attorney General working group that would be required by the TRACED Act specifically calls for including representatives from the Department of State to aid in these efforts. The FCC has also stated that the current 1-year the statute of limitations for violations of TCPA often does not provide sufficient time for the agency to complete investigations involving complex robocalling.[32] The TRACED Act would increase the statute of limitations for TCPA violations from 1 year to 3 years

---

[26] Peterson testimony; *see also* "Illegal Robocalls: Calling All to Stop the Scourge," hearing before the Subcommittee on Communications, Technology, Innovation, and the Internet of the Senate Committee on Commerce, Science, and Transportation, 116th Congress (2019) (testimony of Kevin Rupy on behalf of USTelecom–The Broadband Association) (*https://www.commerce.senate.gov/public/_cache/files/855a4376-1552-4331-9b80-60743250490e/37FA3F42A63B5BA5E8DE1CF0FC983424.04-11-2019rupy-testimony.pdf*) (Rupy testimony).

[27] Thune comments.

[28] Peterson testimony.

[29] Rupy testimony.

[30] FCC report at 14.

[31] Consolidated Appropriations Act, 2018, Public Law 115–141; section 503.

[32] FCC report at 14.

for intentional violations, as discussed below, which would enable the FCC to better pursue bad actors.

The TRACED Act is designed to respond to the scourge of illegal robocalls. The legislation would help to substantially increase the penalties for illegal robocalls with intent. The bill would provide stronger tools to combat illegal robocalls and ensure that industry and regulators have the tools and resources needed to address changing technologies. The TRACED Act has broad support: more than 60 Senators are cosponsors of the bill; Attorneys General from all 50 States, the District of Columbia, and three U.S. territories have expressed support for the TRACED Act, as have all Commissioners from both the FCC and FTC; and consumer organizations, including Consumer Reports and AARP, and telecommunications industry groups, including CTIA and US Telecom, have called for passage of the bill.

SUMMARY OF MAJOR PROVISIONS

S. 151 would do the following:

(1) Provide the FCC with authority to issue additional civil penalties of up to $10,000 per call on those individuals who intentionally violate section 227(b) of the Communications Act of 1934.

(2) Increase the FCC's ability to initiate enforcement actions against those entities that make illegal robocalls with the intention to violate the law by extending the statute of limitations for such violations from 1 year to 3 years, and eliminates the citation requirement for such violations.

(3) Direct the FCC to require voice service providers to implement the STIR/SHAKEN authentication framework within 18 months of enactment if providers have not already taken certain steps to do so, while allowing the FCC to extend the deadline in the event of undue hardship.

(4) Direct the FCC to study the implementation of STIR/SHAKEN and the efficacy of the STIR/SHAKEN authentication framework every 3 years and report findings on actions taken to revise or replace STIR/SHAKEN if the FCC determines it is in the public interest.

(5) Require the FCC to develop rules pertaining to a safe harbor for voice service providers that inadvertently block legitimate callers under a STIR/SHAKEN protocol and have used reasonable care, and allowing parties adversely affected to verify the authenticity of their calls.

(6) Require the FCC to conduct a rulemaking regarding methods to protect subscribers from receiving unwanted calls or text messages that use an unauthenticated number.

(7) Direct the Attorney General to convene an interagency working group to study the prosecution of violations of section 227(b) of the Communications Act of 1934 and to provide a report on its findings within 270 days of enactment.

(8) Direct the FCC to conduct a rulemaking to consider ways to modify FCC policies to reduce access to numbers by potential violators within 180 days of enactment.

LEGISLATIVE HISTORY

S. 151, the TRACED Act, was introduced on January 16, 2019, by Senator Thune (for himself and Senator Markey) and was referred to the Committee on Commerce, Science, and Transportation of the Senate. As of May 20, 2019, S. 151 has 81 additional cosponsors. On April 3, 2019, the Committee met in open Executive Session and, by voice vote, ordered S. 151 reported favorably with an amendment in the nature of a substitute. The Committee also adopted by voice vote an amendment by Senator Moran that would require the FCC to submit an annual report to Congress detailing its enforcement activities related to the laws, regulations, and policies concerning robocalls and spoofed calls, and specifying the number of complaints received, complaints issued, and notices of apparent liability issued by the FCC.

The House of Representatives has an identical bill, H.R. 1602, the Telephone Robocall Abuse Criminal Enforcement and Deterrence Act, which was introduced on March 7, 2019, by Representative Kustoff (for himself and Representative Posey) and was referred to the Committee on Energy and Commerce of the House of Representatives.

Similar legislation, S. 3655, the Telephone Robocall Abuse Criminal Enforcement and Deterrence Act, was previously introduced and referred to the Committee in the 115th Congress.

On April 11, 2019, the Committee's Subcommittee on Communications, Technology, Innovation, and the Internet held a hearing titled "Illegal Robocalls: Calling All to Stop the Scourge," during which the subcommittee received testimony regarding the need to provide consumers relief from illegal robocalls and ways to improve law enforcement tools to combat robocalls.[33]

On April 18, 2018, the full Committee held a hearing titled "Abusive Robocalls and How We Can Stop Them." This hearing examined the problem of malicious spoofing and abusive robocalls designed to defraud consumers, as well as measures being taken by government and industry to protect consumers.

On May 18, 2016, the full Committee held a hearing titled "The Telephone Consumer Protection Act at 25: Effects on Consumers and Business." This hearing examined the TCPA, the limits it imposed on robocalls, and how the FCC had applied the TCPA to new technologies and practices popularized since adoption of the TCPA.

ESTIMATED COSTS

In accordance with paragraph 11(a) of rule XXVI of the Standing Rules of the Senate and section 403 of the Congressional Budget Act of 1974, the Committee provides the following cost estimate, prepared by the Congressional Budget Office:

[33] "Illegal Robocalls: Calling All to Stop the Scourge," hearing before the Subcommittee on Communications, Technology, Innovation, and the Internet of the Senate Committee on Commerce, Science, and Transportation, 116th Congress (2019).

S. 151, TRACED Act

As ordered reported by the Senate Committee on Commerce, Science, and Transportation on April 3, 2019

By Fiscal Year, Millions of Dollars	2019	2019-2024	2019-2029
Direct Spending (Outlays)	0	*	*
Revenues	0	*	*
Deficit Effect	0	*	*
Spending Subject to Appropriation (Outlays)	0	*	n.e.

Pay-as-you-go procedures apply?	Yes	**Mandate Effects**	
Increases on-budget deficits in any of the four consecutive 10-year periods beginning in 2030?	No	Contains intergovernmental mandate?	No
		Contains private-sector mandate?	Yes, Cannot Determine Costs

n.e. = not estimated; * = between -$500,000 and $500,000.

S. 151 would authorize the Federal Communications Commission (FCC) to levy additional civil penalties on people who intentionally violate restrictions on the use of automated telephone equipment (that is, illegal robocallers and spoofers).[1] In addition, S. 151 would extend the period in which intentional violators are subject to enforcement, and the FCC would be required to report to the Congress annually on its enforcement.

The bill also would direct the FCC to require voice service providers (VSPs) to implement—within 18 months of enactment—the framework known as STIR/SHAKEN (secure telephone identity revisited and signature-based handling of asserted information using tokens) to authenticate caller ID in their Internet protocol networks. The FCC would be required to assess the implementation and efficacy of the STIR/SHAKEN framework and periodically report to the Congress.

S. 151 also would direct the Department of Justice to form an interagency working group to study prosecutions related to restrictions on the use of automated telephone equipment and report the findings to the Congress.

Budgetary Effects

CBO estimates that additional penalties collected under S. 151, which are recorded in the budget as revenues, would be insignificant because it would probably be difficult to collect assessed penalties.

Using information from the FCC, CBO estimates that the agency's cost to implement the bill would total $1 million over the 2019–2024 period. However, because the FCC is authorized to collect fees sufficient to offset its regulatory costs, CBO estimates that the net cost would be negligible, assuming appropriation actions consistent with that authority.

CBO also estimates that the cost of the operating an interagency working group would not be significant and would be subject to the availability of appropriated funds. The only exception would be the

[1] Robocallers use automatic dialing systems or artificial or prerecorded voices to place calls without the recipients' consent. Spoofers disguise their identities by altering or manipulating information shown on caller ID. Both actions are subject to enforcement by the FCC.

costs associated with the Consumer Financial Protection Bureau's participation in the working group. Any spending by the bureau, which CBO estimates would not be significant, would be considered mandatory.

Private-Sector Mandates

S. 151 contains private-sector mandates as defined in the Unfunded Mandates Reform Act (UMRA). CBO cannot determine whether those mandates' aggregate costs would exceed the UMRA threshold ($164 million in 2019, adjusted annually for inflation).

Under current law, the FCC has encouraged VSPs to develop call authentication procedures that are equivalent to the STIR/SHAKEN framework by November 2019. If VSPs do not voluntarily meet that standard within a year of enactment, the bill would direct the FCC to require them to adopt the STIR/SHAKEN framework within 18 months of enactment. The mandate's cost would be the expenses incurred by VSPs to match or adopt the framework as established through FCC regulation. Because CBO cannot anticipate the rate or degree of compliance at the one-year mark, we cannot determine whether the mandate's costs would exceed the private-sector threshold.

S. 151 would impose an additional private-sector mandate by removing a private right of action. The bill would limit the right of plaintiffs to file suit against certain VSPs for unintended or inadvertent blocking of calls. The cost of the mandate would be the forgone net value of awards and settlements that would have been granted for such claims in the absence of the bill. CBO has no basis on which to estimate the number of possible lawsuits that would be precluded by the bill and cannot predict the amount of potential forgone settlements. Therefore, we cannot determine whether the cost of the mandate would exceed the annual threshold.

Finally, if the FCC increased fees to offset the costs of implementing activities required by the bill, the cost of an existing private-sector mandate also would increase. Using information from the FCC, CBO estimates that the increase would total about $1 million over the 2019–2024 period.

The CBO staff contacts for this estimate are David Hughes (for federal costs) and Rachel Austin (for mandates). The estimate was reviewed by H. Samuel Papenfuss, Deputy Assistant Director for Budget Analysis.

REGULATORY IMPACT STATEMENT

In accordance with paragraph 11(b) of rule XXVI of the Standing Rules of the Senate, the Committee provides the following evaluation of the regulatory impact of the legislation, as reported:

NUMBER OF PERSONS COVERED

The number of persons covered by this legislation should be consistent with current levels already regulated under the TCPA and the Communications Act of 1934.

ECONOMIC IMPACT

S. 151 is not expected to have an adverse impact on the Nation's economy. Rather, the legislation would promote government and

commercial efforts to reduce one of the largest consumer complaints. By eliminating scams and time-wasting illegal and unwanted robocalls, the legislation should significantly reduce economic inefficiencies associated with those calls, as well as combating fraud and other malicious and costly activity caused by such calls.

PRIVACY

S. 151 would further the privacy protections of the TCPA by helping to reduce the number of illegal robocalls and associated fraud.

PAPERWORK

The Committee does not anticipate a major increase in paperwork burdens resulting from the passage of this legislation, including with respect to the new obligations on voice service providers to adopt call authentication technologies. The bill would require reports to Congress on the steps taken nationally toward adoption of call authentication and on the work of a new interagency working group on preventing robocalls.

CONGRESSIONALLY DIRECTED SPENDING

In compliance with paragraph 4(b) of rule XLIV of the Standing Rules of the Senate, the Committee provides that no provisions contained in the bill, as reported, meet the definition of congressionally directed spending items under the rule.

SECTION-BY-SECTION ANALYSIS

Section 1. Short title.

This section would provide that the legislation may be cited as the "Telephone Robocall Abuse Criminal Enforcement and Deterrence Act" or the "TRACED Act."

Section 2. Forfeiture.

Subsection (a) would amend section 227 of the Communications Act of 1934 ("Communications Act") to add a new subsection (b)(4). Subparagraph (A) of that new subsection would provide that any person that is determined by the Commission, in accordance with paragraph (3) or (4) of section 503(b) of the Communications Act, to have violated any provision of section 227(b) would be liable to the United States for a forfeiture penalty pursuant to sections 503(b)(1) and 503(b)(2) of the Act. The amount of the forfeiture penalty determined under this new subparagraph shall be determined in accordance with subparagraphs (A) through (F) of section 503(b)(2).

Subparagraph (B) of that new subsection would provide that for violations of section 227(b) where there was the intent to cause such violation, the bill would provide that the person who committed such violation would be subject to an enhanced penalty. The amount of that enhanced forfeiture penalty determined under this new subparagraph would be equal to an amount determined in accordance with subparagraphs (A) through (F) of section 503(b)(2), plus an additional amount not to exceed $10,000. The new sub-

section (b)(4) would include a rule of construction providing that the Commission may not impose a forfeiture on a person under both subparagraphs (A) and (B) for the same conduct.

Subsection (a) would further provide that any forfeiture penalty determined under section 2 would be recoverable under section 504(a) of the Communications Act. It also would specify that no forfeiture liability shall be determined under subparagraph (A) or (B) against any person unless such person receives the notice required by paragraph (3) or (4) of section 503(b) of the Communications Act.

The FCC currently has a 1-year statute of limitations for violations of restrictions on the use of automatic telephone dialing systems. Subsection (a) would give the FCC an additional 2 years to pursue intentional violations of restrictions on the use of automatic telephone dialing systems, and would allow the FCC to impose additional fines for such violations.

Finally, subsection (a) would revise section 227(h) of the Communications Act to direct the FCC to prepare an annual report to Congress on its enforcement of laws, regulations, and policies related to robocalls and spoofed calls. The report must include the following:

(1) the number of complaints received that year;

(2) the number of citations issued by the Commission to enforce laws, regulations, and policies related to robocalls and spoofed calls;

(3) the number of notices of apparent liability issued related to such laws, regulations, and policies; and

(4) for each notice of apparent liability, the proposed penalty, the person to whom the notice was issued, and status.

Subsection (b) would state that amendments made by this section shall not affect any action or proceeding commenced before and pending on the date of enactment.

Subsection (c) would direct the FCC to adopt rules implementing this section not later than 270 days after enactment of this Act.

New subsection 227(b)(4)(A) would make clear that the FCC may impose a penalty against any entity, regardless of whether or not it is a licensee or common carrier, that violates section 227(b), without first having to issue a citation. In addition, new subsection 227(b)(4)(B) augments existing penalties against those who intentionally violate the TCPA. Therefore, this new subsection provides the FCC with the authority to impose a penalty of up to $10,000 per intentional unlawful robocall, in addition to the forfeiture penalty amount that may be imposed pursuant to section 503(b) of the Communications Act of 1934, as amended.

The FCC currently has a 1-year statute of limitations for violations of restrictions on the use of automatic telephone dialing systems. The TRACED Act would allow the FCC an additional 2 years to pursue intentional violations of restrictions on the use of automatic telephone dialing systems, and would allow the FCC to impose additional fines for such violations. The Committee intends that the changes made by this section would not in any way limit consumers' private rights of action or existing FCC authority to pursue violations of restrictions on use of telephone equipment under 47 U.S.C. 503(b)(1). Additionally, the TRACED Act is not intended to change the existing FCC rules or the enforcement process

or penalties applicable to good-faith calls made by legitimate businesses as permitted under the provisions of section 227 of the Communications Act.

The Commission has and would retain in full the ability to penalize willful or repeated failure to comply with Commission rules; the TRACED Act would supplement this ability with a 2-year extension for intentional violations. The Committee understands that in the past, the Commission has determined that "willful," as used in section 503(b)(1) of the Communications Act, means "the 'conscious and deliberate commission or omission of [any] act, irrespective of any intent to violate' the law."[34] The Commission concluded "[w]hether [the Company] intended to violate the TCPA is not relevant to determining whether the Company's conduct was willful. [The Company] willfully committed the act of making prerecorded message calls—a service for which it received financial compensation from its clients—and those calls violated the TCPA. [The Company's] violations were therefore willful."[35] Although the Commission would continue to be able to pursue violations—irrespective of any intent to violate-under 47 U.S.C. 227(b)(4)(A), the additional 2 years provided by the TRACED Act would be limited to 47 U.S.C. 227(b)(4)(B)—violations with the intent to cause such violation.

By limiting the extended enforcement period to "violations with the intent to cause such violation," the TRACED Act would allow the Commission additional time to pursue the worst of the worst: scammers and lead-generation mills intentionally violating restrictions on the use of automatic telephone dialing systems. Merely having "committed the act [that] violated the TCPA" would not be sufficient. For example, making a call using an automatic telephone dialing system without having updated a calling list to remove customers that have changed numbers or that revoked consent to receive otherwise prohibited calls would not reach the intent standard necessary for action pursuant to 47 U.S.C. 227(b)(4)(B). Rather, the calling party must knowingly use an automatic telephone dialing system to intentionally place calls to covered numbers without a reasonable basis for believing it had the necessary consent to call. It must also intend to violate the other applicable legal requirements, including any such requirements set forth in the TCPA's statutory exceptions and the regulatory exemptions and clarifications issued by the FCC relating to the TCPA.

If a caller intentionally uses an automatic telephone dialing system to call randomly generated numbers, sequential numbers (i.e., dialing the next ordinal number), or numbers according to a formula (e.g., every third number or numbers divisible by seven) without a reasonable basis to conclude that the intended recipient had consented to receive such calls, that action would constitute the intent to cause a violation, as long as the intent requirement was satisfied for the other elements of the TCPA. Similarly, if a caller uses an automatic telephone dialing system in violation of the restrictions in 47 U.S.C. 227(b), and in making those calls spoofs its number in violation of 47 U.S.C. 227(e), the spoofing would demonstrate intent to cause violations pursuant to 47 U.S.C. 227(b)(4)(B).

---

[34] Dialing Services LLC Forfeiture Order, 32 FCC Rcd. 6192, 6203, at para 30 (2017), (citing 47 U.S.C. 312(f)(1)) (emphasis in original) (*https://docs.fcc.gov/public/attachments/FCC-17-97A1.pdf*).

[35] Id.

The Committee recognizes that the phrasing of this standard is not a common phrasing in the U.S. Code, and is written specifically in light of the need to overcome the Commission's interpretation of "willful," to ensure that this new enhanced enforcement authority is limited to truly intentional violations. The Committee intends for the Commission and the courts to interpret this standard in a straightforward manner consistent with the guidance expressed here.

It would be an affirmative defense to an action pursuant to 47 U.S.C. 227(b)(4)(B) to demonstrate a practice of having prior business relationships with the overwhelming majority of intended call recipients.

The Act would not apply the heightened intent standard to violations other than violations of 47 U.S.C. 227(b).

Section 3. Call authentication.

Subsection (a) would provide definitions for "STIR/SHAKEN authentication framework" and "voice service" as used in this section.

Subsection (b) would direct the FCC to require a provider of voice service to implement the STIR/SHAKEN authentication framework in the Internet-protocol networks of voice service providers within 18 months of enactment. The FCC shall not take action against a voice provider, though, if it determines that a provider of voice service, not later than 12 months after enactment:

(1) has adopted the STIR/SHAKEN authentication framework;

(2) has agreed to participate with other voice service providers in the STIR/SHAKEN authentication framework;

(3) has begun implementation of the STIR/SHAKEN authentication framework; and

(4) will be capable of fully implementing the STIR/SHAKEN authentication framework not later than 18 months after enactment.

Subsection (b) also would direct the FCC, within 12 months of enactment, to report on the determination required under paragraph (b)(2). The report must include analysis of the extent to which providers of voice services have implemented the STIR/SHAKEN authentication framework and an assessment of the efficacy of the STIR/SHAKEN authentication framework in addressing all aspects of call authentication.

Subsection (b) also would require the FCC—within 3 years of enactment and every 3 years thereafter—to analyze the efficacy of the authentication framework implemented under this section and to revise or replace the call authentication framework under this section if the FCC determines it is in the public interest to do so. The FCC would also be required to report on the findings of these analyses and any actions to revise or replace the call authentication under subparagraph (4)(b).

Efforts to combat illegal robocalls and Caller ID scams are not intended to dampen competition or innovation in the U.S. communications marketplace. The success of the STIR/SHAKEN framework's implementation across U.S. voice networks will depend, in part, on making solutions available for the variety of calling technologies and business models. As part of its implementation report, the Commission shall investigate and report on the success of efforts to develop standards to enable STIR/SHAKEN implementa-

tion for the various calling technologies and business models, such as the development of a TN-PoP solution for outbound-only calling services or its successor.

Subsection (b) also would allow the FCC to extend any deadline for the implementation of a call authentication framework required under this section by 12 months or a further amount of time as the FCC determines necessary if the FCC determines that purchasing or upgrading equipment to support call authentication, or the lack of availability of equipment, would constitute a substantial hardship for a provider or category of providers of voice services.

In its initial form, STIR/SHAKEN may not function properly with certain calling technologies and in certain scenarios, such as outbound-only calling technologies where the service provider does not assign individual telephone numbers to outbound callers. The development of a solution will require broad industry participation, and the FCC should encourage such participation. The Commission should encourage Alliance for Telecommunications Industry Solutions (ATIS) members, including key industry stakeholders, to develop without undue delay, a call authentication solution such as TN-PoP or a similar extension of STIR/SHAKEN that will provide an opportunity for such calling technologies to receive the highest level of attestation for outbound calls. If such a standard is not readily available but development is proceeding in a reasonable and timely manner, the Commission may consider the lack of an industry-standard approach to signing that would permit these companies to obtain highest level attestation for their outbound calls to present a substantial hardship and should, if it is in the public interest to do so, grant an extension of the implementation deadline to legitimate voice service providers using such technologies, if those providers demonstrate reasonable efforts to minimize caller ID fraud and readiness to implement a technological solution once it becomes available. Similarly, the Commission should monitor the pace with which equipment vendors upgrade their products to enable STIR/SHAKEN signing and should consider granting an extension, if consistent with the public interest to do so, to any class of service providers whose implementation of STIR/SHAKEN is hampered by an inability to procure the necessary equipment.

Subsection (c) would direct the FCC to promulgate a series of rules related to the use of call authentication technologies. Specifically, these rules must establish when a provider of voice service may block a voice call based on information provided by a call authentication framework. The rules would also establish a safe harbor shielding a provider of voice service from liability for unintended or inadvertent blocking of calls, or for the unintended or inadvertent misidentification of the level of trust for individual calls based on information provided by the call-authentication framework. The rules would also establish a process to permit a calling party adversely affected by the information provided by the authentication framework to verify the authenticity of the calling party's calls. As part of the creation of this process the Committee believes that the Commission should consider what information can be provided to a caller so that the caller can determine why it has been adversely affected by call authentication, but should not provide in-

formation that would facilitate frustration of call authentication technologies.

Paragraph (c)(2) would direct the FCC to consider three elements when limiting the liability of a provider based on the extent to the which the provider:

(1) blocks or identifies calls based on the information provided by the authentication framework;

(2) implements procedures based on the information provided by the authentication framework; and

(3) uses reasonable care.

In determining under what circumstances to provide a safe harbor for inadvertently blocking legitimate calls, this section outlines a minimum set of considerations in order to limit any potentially adverse impact of such action on voice service providers and consumers. These considerations are not intended to supplant the factors to which the Commission is more generally instructed to adhere to in the Communications Act. In establishing a safe harbor, the Commission's consideration of more general factors should include, among other things, the potential effect on different technologies and categories of voice communications providers including those who do not qualify as providers of voice services and the potential effect on subscribers including those who wish to receive all inbound calls.

When establishing the rules for when a voice service provider may block a voice call, the Committee expects the FCC to consider the benefits of protecting consumers from illegal robocalls, and also the burden on callers and consumers in allowing voice service providers to block calls without providing prior or contemporary notice to the caller and an opportunity for the caller to rebut a blocking determination. When establishing the process by which callers may have their calls unblocked, the FCC should consult call originators in addition to voice service providers. The safe harbor should not be used to support blocking or mislabeling calls from legitimate businesses.

The process established by the FCC should require voice service providers to unblock improperly blocked calls in as timely and efficient a manner as reasonable. The FCC should ensure that: (1) legitimate businesses and institutions conveying information to consumers are not unreasonably impacted by the TRACED Act or voice service providers' implementation of STIR/SHAKEN; and (2) the authentication and unblocking process under STIR/SHAKEN is not unduly burdensome to and does not unreasonably negatively impact legitimate call originators. Although blocking may be warranted in certain instances, the Commission should require that voice service providers provide their subscribers with a meaningful opportunity to understand that call filtering or blocking of certain inbound calls to their telephone number is being employed and should consider the feasibility of providing subscribers a meaningful and persistent opportunity to reject such blocking.

Subsection (d) would clarify that nothing in this section precludes the FCC from initiating a rulemaking pursuant to its existing authority.

Section 4. Protections from spoofed calls.

This section would direct the FCC to initiate a rulemaking within 1 year of enactment to help protect a subscriber from receiving unwanted calls or text messages from a caller using an unauthenticated number.

The FCC must consider the following when promulgating rules pursuant to this section:

(1) the GAO report on combating the fraudulent provision of misleading or inaccurate caller identification required by the Consolidated Appropriations Act 2018 (P.L. 115–141);

(2) the best means of ensuring that a subscriber or provider has the ability to block calls from a caller using an unauthenticated North American Numbering Plan number;

(3) the impact on the privacy of a subscriber from unauthenticated calls;

(4) the effectiveness in verifying the accuracy of caller-identification information; and

(5) the availability and cost of providing protection from the unwanted calls or text messages described in this section.

The various considerations seek to ensure that the rules promulgated by the Commission are designed to ensure the Commission considers possible harm to competition and consumer trust in the telephone network. These considerations are a minimum set of considerations and the Commission should also consider: the benefits of measures designed to protect subscribers from receiving unwanted calls; the effect of such measures on the provision of voice communications by entities that do not qualify for full attestation under the STIR/SHAKEN standard; the effect on different voice technologies and business models; the effect of blocking or failing to block on the continued reliability of the public switched telephone network; and mechanisms to minimize potential harms. Measures designed to protect subscribers from receiving unwanted calls or texts on the basis of the call authentication framework can produce unwanted negative outcomes or inadvertent harms. For example, call blocking or filtering could disproportionately affect categories of providers excluded from STIR/SHAKEN—such as non-interconnected VoIP, international calls, and TDM calls—and this could harm competition as well as the perceived validity of the authentication system. If subscribers begin to question the validity of STIR/SHAKEN, because it results in over-blocking or over-filtering of calls, there is a danger that subscribers could ignore the information it supplies, notwithstanding considerable industry investment in the framework.

In considering the best means of ensuring that a subscriber or provider has the ability to block calls from a caller using an unauthenticated North American Numbering Plan number, the Commission should ensure that its efforts consider to the extent possible the Government Accountability Office report required by section 503(c) of division P of the Consolidated Appropriations Act 2018 (P.L. 115–141), and the consumer education materials developed pursuant to section 503(b) of that law.

Section 5. Interagency working group.

This section directs the Attorney General, in consultation with the Chairman of the FCC, to convene an interagency working

group to study prosecution of robocall violations. The section prescribes the working group's study to include whether, and if so how, any Federal laws, including regulations, policies, and practices, or budgetary or jurisdictional constraints, inhibit the prosecution of such violations. The study would also identify existing and potential Federal policies and programs that encourage and improve coordination among Federal departments and agencies and States, and between States, in the prevention and prosecution of robocall violations.

The working group should also consider collection of fines imposed by the FCC for robocall violations.

Paragraph (b)(3) would direct the working group to identify existing and potential international policies and programs that encourage and improve coordination between countries in the prevention and prosecution of robocall violations.

Paragraph (b)(4) would also direct the working group to study the following:

(1) if any additional resources are necessary for the Federal prevention and prosecution of criminal violations of the Act;

(2) whether to establish memoranda of understanding regarding the prevention and prosecution of such violations between the States, the States and Federal Government, and the Federal Government and a foreign government;

(3) whether to establish a process to allow States to request Federal subpoenas from the FCC;

(4) whether extending civil enforcement authority to the States would assist in the successful prevention and prosecution of such violations;

(5) whether increased forfeiture and imprisonment penalties are appropriate;

(6) whether regulation of any entity that enters into a business arrangement with a common carrier for the specific purpose of carrying, routing, or transmitting a call that constitutes such a violation would assist in the successful prevention and prosecution of such violations; and

(7) the extent to which any Department of Justice policies to pursue the prosecution of violations causing economic harm, physical danger or erosion of an inhabitant's peace of mind and sense of security inhibits the prevention or prosecution of any such violations.

Paragraph (c) would direct the composition of the working group to include possible members from the Department of Commerce, the Department of State, the Department of Homeland Security, the FCC, the FTC, and the Bureau of Consumer Financial Protection.

Paragraph (d) would direct the working group to consult with non-Federal stakeholders, such as those the Attorney General determines to have relevant expertise.

Paragraph (e) would require the working group to report within 270 days of enactment any recommendations regarding the prevention and prosecution of violations and what progress Federal departments and agencies have made in implementing those recommendations.

The Commission should consider establishing a task force within the Enforcement Bureau to advise the Commission on the prevention of robocall fraud.

Section 6. Access to number resources.

This section directs the FCC to commence a proceeding within 180 days of enactment to determine whether FCC policies regarding access to number resources could be modified to help reduce access to numbers by potential violators of section 227(b). This section further directs the FCC to implement regulations to achieve the goal of reducing such access if it determines policy modifications are necessary.

This section would also impose liability under section 503 of the Communications Act on any person who knowingly, through an employee, agent, officer, or otherwise, directly or indirectly, by or through any means or device, is a party to obtaining number resources, including number resources for toll free and non-toll free telephone numbers, from a common carrier regulated under title II in violation of a regulation promulgated by the Commission under this section.

In considering whether the Commission's rules regarding access to number resources can be modified to help reduce assess to numbers by potential perpetrators of violations of section 227(b), the Commission should consider implications for innovation and the voice communication economy. For example, modification of policies for access to number resources could increase the difficulty for non-offenders to obtain U.S. telephone numbers, and requirements such as in-person presentation of documents or identity verification tend to favor non-Internet-based companies or those with physical lines over those who do business via the Internet or use newer technologies. Similarly, residency requirements for telephone numbers may reduce downward competitive pressure on international voice calling rates. Therefore, at a minimum, the Commission should consider, among other things, the direct or indirect impact that any modifications might have on competition in and rates for voice communications, including international calling, and the impact that any modifications might have on different voice technologies and business models, as well as reasonable measures that could be taken to reduce potential negative impacts.

CHANGES IN EXISTING LAW

In compliance with paragraph 12 of rule XXVI of the Standing Rules of the Senate, changes in existing law made by the bill, as reported, are shown as follows (existing law proposed to be omitted is enclosed in black brackets, new material is printed in italic, existing law in which no change is proposed is shown in roman):

COMMUNICATIONS ACT OF 1934

[47 U.S.C. 227]

SEC. 227. RESTRICTIONS ON THE USE OF TELEPHONE EQUIPMENT.

(a) * * *

(b) RESTRICTIONS ON THE USE OF AUTOMATED TELEPHONE EQUIPMENT.—

(1) * * *

(4) CIVIL FORFEITURE.—

(A) IN GENERAL.—Any person that is determined by the Commission, in accordance with paragraph (3) or (4) of section 503(b), to have violated any provision of this subsection shall be liable to the United States for a forfeiture penalty pursuant to section 503(b)(1). The amount of the forfeiture penalty determined under this subparagraph shall be determined in accordance with subparagraphs (A) through (F) of section 503(b)(2).

(B) VIOLATION WITH INTENT.—Any person that is determined by the Commission, in accordance with paragraph (3) or (4) of section 503(b), to have violated this subsection with the intent to cause such violation shall be liable to the United States for a forfeiture penalty. The amount of the forfeiture penalty determined under this subparagraph shall be equal to an amount determined in accordance with subparagraphs (A) through (F) of section 503(b)(2) plus an additional penalty not to exceed $10,000.

(C) RECOVERY.—Any forfeiture penalty determined under subparagraph (A) or (B) shall be recoverable under section 504(a).

(D) PROCEDURE.—No forfeiture liability shall be determined under subparagraph (A) or (B) against any person unless such person receives the notice required by paragraph (3) or (4) of section 503(b).

(E) STATUTE OF LIMITATIONS.—No forfeiture penalty shall be determined or imposed against any person—

(i) under subparagraph (A) if the violation charged occurred more than 1 year prior to the date of issuance of the required notice or notice of apparent liability; and

(ii) under subparagraph (B) if the violation charged occurred more than 3 years prior to the date of issuance of the required notice or notice of apparent liability.

(F) RULE OF CONSTRUCTION.—Notwithstanding any law to the contrary, the Commission may not determine or impose a forfeiture penalty on a person under both subparagraphs (A) and (B) based on the same conduct.

(c) * * *

[(h) JUNK FAX ENFORCEMENT REPORT.—The Commission shall submit an annual report to Congress regarding the enforcement during the past year of the provisions of this section relating to sending of unsolicited advertisements to telephone facsimile machines, which report shall include—

[(1) the number of complaints received by the Commission during such year alleging that a consumer received an unsolicited advertisement via telephone facsimile machine in violation of the Commission's rules;

[(2) the number of citations issued by the Commission pursuant to section 503 during the year to enforce any law, regu-

lation, or policy relating to sending of unsolicited advertisements to telephone facsimile machines;

[(3) the number of notices of apparent liability issued by the Commission pursuant to section 503 during the year to enforce any law, regulation, or policy relating to sending of unsolicited advertisements to telephone facsimile machines;

[(4) for each notice referred to in paragraph (3)—

[(A) the amount of the proposed forfeiture penalty involved;

[(B) the person to whom the notice was issued;

[(C) the length of time between the date on which the complaint was filed and the date on which the notice was issued; and

[(D) the status of the proceeding;

[(5) the number of final orders imposing forfeiture penalties issued pursuant to section 503 during the year to enforce any law, regulation, or policy relating to sending of unsolicited advertisements to telephone facsimile machines;

[(6) for each forfeiture order referred to in paragraph (5)—

[(A) the amount of the penalty imposed by the order;

[(B) the person to whom the order was issued;

[(C) whether the forfeiture penalty has been paid; and

[(D) the amount paid;

[(7) for each case in which a person has failed to pay a forfeiture penalty imposed by such a final order, whether the Commission referred such matter for recovery of the penalty; and

[(8) for each case in which the Commission referred such an order for recovery—

[(A) the number of days from the date the Commission issued such order to the date of such referral;

[(B) whether an action has been commenced to recover the penalty, and if so, the number of days from the date the Commission referred such order for recovery to the date of such commencement; and

[(C) whether the recovery action resulted in collection of any amount, and if so, the amount collected.]

(h) TCPA ENFORCEMENT REPORT.—The Commission shall submit an annual report to Congress regarding the enforcement during the preceding year of laws, regulations, and policies relating to robocalls and spoofed calls, which report shall include—

(1) the number of complaints received by the Commission during the year alleging that a consumer received a robocall or spoofed call;

(2) the number of citations issued by the Commission pursuant to section 503 during the year to enforce any law, regulation, or policy relating to a robocall or spoofed call;

(3) the number of notices of apparent liability issued by the Commission pursuant to section 503 during the year to enforce any law, regulation, or policy relating to a robocall or spoofed call; and

(4) for each notice referred to in paragraph (3)—

(A) the amount of the proposed forfeiture penalty involved;

(B) the person to whom the notice was issued; and

(C) the status of the proceeding.

○