

Alert | Technology, Media & Telecommunications



January 2020

TRACED Act Subjects Robocallers to Increased Penalties, Outlines Regulatory and Reporting Requirements to Deter Violations

On Dec. 31, 2019, President Trump signed into law the [Pallone-Thune Telephone Robocall Abuse Criminal Enforcement and Deterrence Act \(TRACED Act\)](#). The TRACED Act amends the Telephone Consumer Protection Act (TCPA) to increase the monetary forfeitures for violations of the TCPA and extends the applicable statute of limitations for intentional violations.¹ The TRACED Act also instructs the FCC to (1) promulgate rules that will strengthen protections against robocalls and the manipulation of caller-identification information to disguise the identity of the actual caller (known as caller-ID spoofing) and (2) submit reports to Congress regarding various issues related to robocalls and efforts to discourage conduct in violation of the TCPA. Finally, the TRACED Act directs the establishment of working groups to focus on the prosecution of robocallers and prevention of robocalls placed to hospitals.

¹ The TCPA and implementing regulations adopted by the Federal Communications Commission (FCC) generally prohibit the use of autodialed, prerecorded or artificial voice calls (commonly known as robocalls) to wireless telephone numbers and the use of prerecorded or artificial voice calls to residential telephone numbers unless the caller has received the prior express consent of the called party (certain calls, such as telemarketing calls, require prior express *written* consent) or is subject to specified exemptions. See 47 U.S.C. § 227; 47 C.F.R. § 64.1200.

Monetary Forfeitures and Statute of Limitations

The TRACED Act amends the section of the TCPA that prohibits robocalling (47 U.S.C. § 227(b)) by explicitly referencing civil monetary forfeitures to be imposed by the FCC as a penalty for violations. Prior to the amendment, the TCPA only identified a private right of action as a remedy for violation of Section 227(b) (although under 47 U.S.C. § 503, the FCC has authority to impose monetary forfeitures for willful or repeated violation of its rules or orders). For persons or entities that are not FCC licensees or common carriers, the forfeiture penalty shall not exceed \$20,489 for each violation, and the amount of any forfeiture assessed for any continuing violation shall not exceed a total of \$153,669 for any single act.² The TRACED Act requires an additional forfeiture penalty (on top of the forfeiture penalty set forth in 47 U.S.C. § 503) not to exceed \$10,000 for intentional violations of the TCPA's robocalling prohibitions. Given that each unlawful call is a violation, forfeiture amounts can be substantial for a robocaller, especially for a robocaller the FCC finds has acted with an intent to violate the law.

The TRACED Act makes two changes to the TCPA that expand the scope of conduct subject to an enforcement action initiated by the FCC. First, for conduct in violation of the TCPA's robocalling prohibitions found to be intentional and for violation of the TCPA's caller ID spoofing prohibitions, the FCC may issue a notice of apparent liability proposing a monetary forfeiture for conduct that occurred within the past four years.³ (The statute of limitations for caller ID spoofing conduct had been two years.) For robocalling violations that are not deemed intentional, a notice of apparent liability may only address conduct that occurred within the prior year (which is the statute of limitations normally applicable to violations of the FCC's rules). Second, all violators of the TCPA's robocalling and caller ID spoofing restrictions, including those violators that do not hold FCC licenses or other authorizations, are subject to receiving a notice of apparent liability from the FCC. Pursuant to the FCC's rules, the FCC must issue a citation to persons or entities that do not hold an FCC authorization as a warning to cease conduct that violates the FCC's rules before the FCC issues a notice of apparent liability. However, the TRACED Act expressly provides that this prior citation requirement is not applicable to robocall and caller ID spoofing violators.

Regulatory and Reporting Requirements

The TRACED Act directs the FCC to engage in several rulemaking, monitoring, and reporting activities as a means to deter robocalling and caller ID spoofing. The TRACED Act also requires the FCC and other governmental agencies to work together to improve robocalling prevention and enforcement efforts.

FCC Regulatory Actions

- **Forfeiture and Statute of Limitations:** FCC must prescribe regulations to implement the forfeiture and statute of limitations changes described above.
- **STIR/SHAKEN Call Authentication:** FCC must require a provider of voice service to implement the STIR/SHAKEN authentication framework⁴ in its internet protocol networks to take reasonable measures to implement an effective call authentication framework in its non-internet protocol

² See 47 U.S.C. § 503(b)(2)(D) as adjusted for inflation pursuant to the Federal Civil Penalties Inflation Adjustment Act Improvements Act of 2015, Public Law 114-74 (129 Stat. 599-600).

³ The FCC may issue a forfeiture order if it finds that the recipient of a notice of apparent liability has not adequately responded to the FCC's allegations. The FCC may also seek to resolve the matter through a consent order, which generally requires the alleged violator to make a voluntary payment, develop a compliance plan, and file compliance reports.

⁴ STIR/SHAKEN authentication framework means the Secure Telephone Identity Revisited and Signature-based Handling of Asserted Information standards proposed by the information and communications technology industry.

networks, unless the FCC determines that voice service providers will meet specified call authentication standards. FCC also must issue call authentication best practices.

- **Unauthenticated Calls:** FCC to commence a rulemaking to protect consumers from receiving unwanted calls from unauthenticated numbers. (The FCC has already initiated such a rulemaking.)
- **Private Consortium to Trace Back Calls:** FCC to establish a process for the registration of a single consortium that conducts private-led efforts to trace back the origin of suspected unlawful robocalls.
- **One-Ring Scams:** FCC to initiate a proceeding to protect called parties from one-ring scams.⁵
- **Call Blocking:** FCC to promulgate rules establishing when a voice services provider may block a call based on a call authentication framework and establishing a safe harbor for unintended or inadvertent call blocking. Service providers may not charge consumers for call blocking.
- **Number Resources:** FCC to commence a proceeding to determine how to modify policies regarding access-to-number resources and to promulgate any necessary regulations.
- **Voluntary Reporting of Violations:** FCC to establish a process that streamlines the ways in which a private entity may voluntarily share that a call was made in violation of the TCPA's robocalling or call ID spoofing prohibitions.
- **Calls to Hospitals:** FCC to establish a Hospital Robocall Protection Group and issue best practices regarding how voice service providers, hospitals, and governments can combat unlawful robocalls to hospitals.

Reports

- **Annual Reports:** FCC to submit annual reports to Congress regarding (1) robocalls and caller ID spoofing and (2) status of efforts to trace back the origin of suspected unlawful robocalls.
- **Attorney General:** FCC Enforcement Bureau to provide evidence of willful, knowing, and repeated robocall violations with an intent to defraud, cause harm, or wrongfully obtain anything of value to the attorney general and submit an annual report to Congress regarding the number and type of robocall violations reported to the attorney general.
- **Other Reports:** FCC to submit various reports to Congress including reports on (1) implementation and efficacy of call authentication frameworks; (2) a reassigned numbers database (to avoid calls without the prior express consent of the called party due to a reassigned number); and (3) the status of the one-ring scam proceeding.
- **Interagency Working Group:** Attorney general to convene an interagency working group to study prosecution of violation of the TCPA's robocalling prohibitions. Group to submit a report to Congress regarding recommendations for the prevention and prosecution of such violations.

Conclusion

The TRACED Act expands the FCC's authority to promulgate rules that establish stronger protections against unlawful robocalls and caller ID spoofing and to enforce the TCPA against all persons and entities that target consumers with such calls. The TRACED Act's substantial rulemaking, best practices, and reporting requirements indicate that Congress views eradication of robocalls and fraudulent caller ID conduct to be a serious matter, and that violators will be subject to enforcement actions. Therefore, it is

⁵ A one-ring scam is "a scam in which a caller makes a call and allows the call to ring the called party for a short duration, in order to prompt the called party to return the call, thereby subjecting the called party to charges." TRACED Act, § 12(d)(1).

essential that any company that utilizes robocalls to contact consumers on their wireless or residential phones understand the federal requirements governing such calls and the sanctions for violation of those requirements, and maintain and follow comprehensive compliance policies and procedures.

If you have questions about the TRACED Act or other questions regarding the TCPA or robocalls, please contact us at your convenience. [Read additional GT Insights on robocall regulation.](#)

Authors

This GT Alert was prepared by **Mitchell F. Brecher** and **Debra McGuire Mercer**. Questions about this information can be directed to:

- [Mitchell F. Brecher](#) | +1 202.331.3152 | brechermt@gtlaw.com
- [Debra McGuire Mercer](#) | +1 202.331.3194 | mercercdm@gtlaw.com
- Or your [Greenberg Traurig](#) attorney

Albany. Amsterdam. Atlanta. Austin. Boca Raton. Boston. Chicago. Dallas. Delaware. Denver. Fort Lauderdale. Germany.[~] Houston. Las Vegas. London.* Los Angeles. Mexico City.+ Miami. Milan.* Minneapolis. Nashville. New Jersey. New York. Northern Virginia. Orange County. Orlando. Philadelphia. Phoenix. Sacramento. San Francisco. Seoul.[∞] Shanghai. Silicon Valley. Tallahassee. Tampa. Tel Aviv.^ Tokyo.* Warsaw.^ Washington, D.C.. West Palm Beach. Westchester County.

*This Greenberg Traurig Alert is issued for informational purposes only and is not intended to be construed or used as general legal advice nor as a solicitation of any type. Please contact the author(s) or your Greenberg Traurig contact if you have questions regarding the currency of this information. The hiring of a lawyer is an important decision. Before you decide, ask for written information about the lawyer's legal qualifications and experience. Greenberg Traurig is a service mark and trade name of Greenberg Traurig, LLP and Greenberg Traurig, P.A. ~Greenberg Traurig's Berlin office is operated by Greenberg Traurig Germany, an affiliate of Greenberg Traurig, P.A. and Greenberg Traurig, LLP. *Operates as a separate UK registered legal entity. +Greenberg Traurig's Mexico City office is operated by Greenberg Traurig, S.C., an affiliate of Greenberg Traurig, P.A. and Greenberg Traurig, LLP. »Greenberg Traurig's Milan office is operated by Greenberg Traurig Santa Maria, an affiliate of Greenberg Traurig, P.A. and Greenberg Traurig, LLP. ∞Operates as Greenberg Traurig LLP Foreign Legal Consultant Office. ^Greenberg Traurig's Tel Aviv office is a branch of Greenberg Traurig, P.A., Florida, USA. ¤Greenberg Traurig Tokyo Law Offices are operated by GT Tokyo Horitsu Jimusho, an affiliate of Greenberg Traurig, P.A. and Greenberg Traurig, LLP. ~Greenberg Traurig's Warsaw office is operated by Greenberg Traurig Grzesiak sp.k., an affiliate of Greenberg Traurig, P.A. and Greenberg Traurig, LLP. Certain partners in Greenberg Traurig Grzesiak sp.k. are also shareholders in Greenberg Traurig, P.A. Images in this advertisement do not depict Greenberg Traurig attorneys, clients, staff or facilities. No aspect of this advertisement has been approved by the Supreme Court of New Jersey. ©2020 Greenberg Traurig, LLP. All rights reserved.*