FCC Adopts Safe Harbors to Encourage Phone Companies to Block Illegal Robocallers

On July 16, 2020, the Federal Communications Commission (FCC) adopted rules to further strengthen protections against illegal and unwanted robocalls.¹ The FCC’s amended rules, which implement portions of the Pallone-Thune Telephone Robocall Abuse Criminal Enforcement and Deterrence Act (TRACED Act), offer telephone service providers two safe harbors from liability for unintended or inadvertent blocking of wanted calls. A detailed discussion of the TRACED Act is contained in GT Alert, “TRACED Act Subjects Robocallers to Increased Penalties, Outlines Regulatory and Reporting Requirements to Deter Violations.”

Over the past several years, the FCC has empowered phone companies to be proactive in blocking unlawful robocalls to their customers. For example, in November 2017, the FCC authorized phone companies to block calls purporting to originate from unassigned, unallocated, or invalid numbers.² In 2019, the FCC clarified that phone companies may block calls to their customers by default where, based on reasonable analytics, the phone companies determine that the calls are unwanted. However, the phone

---

¹ The Telephone Consumer Protection Act (TCPA) (which was amended by the TRACED Act) and the FCC’s implementing regulations 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.

² See 47 C.F.R. § 64.1200(k).
companies are required to allow customers to opt out of call blocking.\(^3\) The TRACED Act directed the FCC to continue its effort to protect customers from illegal and unwanted robocalls, in part, by establishing safe harbors for phone companies that use call blocking.

The FCC adopted two safe harbors to protect phone companies that engage in call blocking to prevent their customers from receiving illegal robocalls. The safe harbors cover the following situations:

- Phone companies that block calls based on reasonable analytics, such as caller ID authentication information. Reasonable analytics must account for information from the STIR/SHAKEN call authentication network.\(^4\)
- Phone companies that block call traffic from “bad actor” upstream voice service providers that pass along illegal robocalls after they were notified of their unlawful actions, but failed to take further action to cease their illegal actions.

The intent of the safe harbors is to encourage phone companies to implement the strongest tools available to block illegal and unwanted robocalls from reaching their customers. The FCC’s amended rules also require phone companies to provide a single point of contact to resolve unintended or inadvertent blocking of wanted calls. In addition, the FCC emphasized the importance of phone companies making reasonable efforts to ensure that critical calls, such as those from Public Safety Answering Points (for example, 911 call centers), are not blocked and that calls to 911 are never blocked. Finally, the FCC announced that it is seeking comment on whether phone companies should be obligated to take further actions to monitor their networks and provide their customers with information about blocked calls for no charge.

**Conclusion**

The FCC’s amended rules, consistent with the TRACED Act, are intended to discourage unlawful robocalling and enable phone companies to take effective steps to protect their customers from unlawful robocalls without risking liability for blocking wanted calls. The FCC’s amended rules also significantly expand phone companies’ call blocking tools, by allowing them to block all traffic from other voice service providers if certain conditions are met regarding those providers’ prior conduct. It is expected that the FCC will continue to work with the telecommunications industry to combat illegal robocalling and to focus enforcement efforts on robocallers that violate the FCC’s rules. Therefore, it is important that companies including telemarketing companies, health care companies, survey research companies, and others, that rely on robocalls to contact consumers understand the federal laws governing such calls and implement procedures to ensure that they comply with those laws and regulations.

**Authors**

This GT Alert was prepared by:

- **Mitchell F. Brecher** | +1 202.331.3152 | brecherm@gtlaw.com
- **Debra McGuire Mercer** | +1 202.331.3194 | mercerdm@gtlaw.com

---

\(^3\) See Advanced Methods to Target and Eliminate Unlawful Robocalls, Call Authentication Trust Anchor, Declaratory Ruling and Third Further Notice of Proposed Rulemaking, 34 FCC Rcd 4876 (2019).

\(^4\) 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.