EVERSHEDS SUTHERLAND

7th Annual TCPA Year-in-Review

Redial: 2020 TCPA Year-in-Review

Analysis of critical issues and trends in TCPA compliance and litigation

Introduction

Eversheds Sutherland is pleased to present our 7th annual TCPA year-in-review report highlighting key TCPA issues and trends.

Did you know?

6 billion

Estimated number of **text messages sent daily** in the US.

100,000

Number of **cell phone numbers** that are **reassigned each day**, according to the FCC.

3,000+

More than **3,000 TCPA lawsuits filed in 2020**.

Eversheds Sutherland industry knowledge and focus

Few industries are immune from TCPA liability. In 2020, the insurance, financial services, energy and health sectors were uniquely affected by TCPA litigation. REDIAL analyzes key legal issues affecting these and other industries.

Eversheds Sutherland tracks daily all TCPA cases filed across the country. This allows us to spot trends and keep our clients focused and informed. We understand the law and our clients' businesses, allowing us to design compliance and risk management programs uniquely suited to our clients' specific needs and to spot issues before they result in litigation. When litigation is filed, Eversheds Sutherland's TCPA team has the depth of experience necessary to efficiently and effectively resolve cases and, when necessary, defend its clients' interests in court.

Why Eversheds Sutherland?

Strength in representing leading companies worldwide

Strength in knowing our clients' businesses

Strength in advising and counseling our clients on TCPA compliance

Strength as trial lawyers in efficiently and effectively representing our clients in class actions filed in state and federal courts across the country

Contents

Supreme Court spotlight

TCPA compliance

Litigation update

Regulatory roundup

Hot issues for 2021

Supreme Court leaves TCPA intact; strikes down exception for government debt collection

The Telephone Consumer Protection Act (TCPA) remains in place, but the exception permitting robocalls for government debt collection has fallen, in a decision by the US Supreme Court addressing the constitutionality of the statute. *Barr v. American Association of Political Consultants*, No. 19-631 (July 6, 2020). Although some commentators had predicted that the Court might use the opportunity to strike down the robocalling provisions of the TCPA as an unconstitutional restriction on the right to free speech, the Court opted for a more limited path. In a case where the justices seemed mostly in agreement on the appropriate outcome, if not the reasoning, six of the justices agreed that the exception for government debt collection—allowing such calls to be made without the same restrictions placed on other calls—was an impermissible content-based distinction under the First Amendment. But there was little appetite for striking down the TCPA in its entirety. Seven of the justices agreed that the appropriate remedy was severing the unconstitutional exception, leaving the remainder of the TCPA in place. Only Justices Gorsuch and Thomas advocated striking down the TCPA's broader restrictions on robocalls.

The Court's decision affirms the judgment of the US Court of Appeals for the Fourth Circuit, which had held that the government-debt exception violated the First Amendment because it was a content-based restriction on speech. In striking down the government-debt exception and affirming the decision below, Justice Kavanaugh delivered the judgment of the Court, reasoning that the TCPA exception for government debt collection was "about as content-based as it gets." By example, Justice Kavanaugh observed that a robocall that saying, "Please pay your government debt" would be legal, but a robocall saying, "Please donate to our political campaign" would be illegal.

More significant than the fall of the exception was what the Court did not do. There was some speculation that the Court would strike down the TCPA in its entirety, thereby invalidating the restrictions on automated dialing that apply to automated and prerecorded calls generally, including political calls. The petitioners argued that the government-debt exception could not be appropriately severed from the statute as a whole, which would imply that the entire statute could be invalidated. Indeed, the petitioners in the lawsuit were political groups that sought relief from the ban on making robocalls for purposes other than government debt collection. Seven justices, however, disagreed that the entire statute should fall. Justice Kavanaugh applied a presumption in favor of severability, reasoning that the remainder of the TCPA is capable of functioning independently and that the exception should be severed. It was also significant to Justice Kavanaugh that, since 1934, the Communications Act in which the TCPA is incorporated has contained an express severability clause.

The argument for striking down the entire statute did find traction with Justices Gorsuch and Thomas. Justice Gorsuch stated that, "In my view, the TCPA's rule against cellphone robocalls is a content-based restriction that fails

With the ruling, the TCPA landscape remains the same as it was under the 4th Circuit's year-old decision, and effectively returns the TCPA's automated call restriction to its pre-2015 existence without the allowance for autodialed or prerecorded calls to collect government-held or -guaranteed debts without prior express consent.

strict scrutiny. The statute is content-based because it allows speech on a subject the government favors (collecting its debts) while banning speech on other disfavored subjects (including political matters)." Justices Gorsuch and Thomas would have granted an injunction against enforcement of the TCPA against the petitioners for other types of robocalls (not government debt collection), a result which would have had the effect of striking down much of the TCPA.

Looking ahead, it seems plausible that the Supreme Court will add another TCPA case to its docket next year, in order to resolve a circuit split over the definition of "automatic telephone dialing system." A petition for certiorari remains pending in an appeal from the US Court of Appeals for the Ninth Circuit on this issue, in *Facebook, Inc. v. Noah Duguid*, Case No. 19-511. The question on appeal is whether the definition of an ATDS encompasses any device that can "store" and "automatically dial" telephone numbers, even if the device does not use a random or sequential number generator. In *Facebook*, the Ninth Circuit applied an expansive definition of an ATDS, which includes any device that can "store" and "automatically dial" telephone numbers, even if the device does not use a random or sequential number generator. In recent months, the Second Circuit has adopted a similar standard, splitting with the Seventh and Eleventh Circuits, which have applied narrower standards.

High Court must right FCC's failure to define autodialers

On July 10, the U.S. Supreme Court granted cert in *Facebook Inc. v. Duguid*, which brings squarely before the court the question of what constitutes an autodialer under the Telephone Consumer Protection Act. The court's decision to grant cert may say as much about the Federal Communications Commission as it does the TCPA.

The question of what constitutes an automatic telephone dialing system, or ATDS, and, therefore, what types of telecommunications devices may be subject to the TCPA, has been at the heart of thousands of lawsuits filed over the past few years.

Over the past year, federal circuit courts have split over the definition of autodialer with the U.S. Court of Appeals for the Second Circuit and U.S. Court of Appeals for the Ninth Circuit aligning to define the term broadly and the U.S. Court of Appeals for the Third Circuit, U.S. Court of Appeals for the Seventh Circuit and U.S. Court of Appeals for the Eleventh Circuit taking a narrow, more business-friendly, view.

Meanwhile, the FCC comment period aimed at developing new rules to add much-needed clarity to the definition of autodialer and the TCPA closed more than a year-and-a-half ago with nothing but deafening silence echoing from the halls of the FCC.

The TCPA defines the term "autodialer" as "equipment which has the capacity— (A) to store or produce telephone numbers to be called, using a random or sequential number generator; and (B) to dial such numbers."

Although this statutory definition may seem clear and unambiguous, the TCPA was passed nearly 30 years ago and, unsurprisingly, does not address contemporary issues presented by current and emerging telecommunications technology. This has led to a long history of twists and turns in the interpretation of this language. Regulators, courts and business have continued to struggle with the foundational TCPA question of what constitutes an automatic telephone dialing system under the statute.

The key question underlying the definition of autodialer is whether the TCPA applies to a dialing system that can call from a stored list of numbers, or whether the TCPA's autodialing restrictions are instead limited to systems that have the capacity for random or sequential number generation, as the plain language of the statue indicates.

Numerous federal appellate courts have considered the issue, and the split in the law is deepening. In light of the TCPA's statutory damages provision that allows for $500 per violation and treble damages for intentional violations, plus attorney fees with no cap on damages, this lack of clarity has been and will continue to be particularly concerning in the context of potential class action liability.

In the middle of this tumult, the FCC issued on June 25 what can best be seen as a milquetoast declaratory ruling barely scratching the surface on defining autodialer, creating a void that the Supreme Court is now poised to fill.

The FCC's June 25 declaratory ruling states the unremarkable proposition that manual dialing is not autodialing — a proposition that should be obvious by common sense but which has been muddied by the general uncertainty surrounding the autodialer definition generally. In response to a petition filed by a coalition of peer-to-peer text messaging services, the FCC ruled that a calling system is not an autodialer if it is "not capable of originating a call or sending a text without a person actively and

The Supreme Court's next term opens in October, and oral argument will be scheduled for a date sometime thereafter. A decision can be expected to be published sometime between the argument and when the terms recesses in early summer 2021.

affirmatively manually dialing each [call or text]." A manual dialing system per this order will "require a person to manually send each text message [or call] one at a time."

Significantly and conspicuously, the FCC's ruling on manual dialing avoided wading into the larger and more significant dispute over systems that can dial from lists of stored numbers, and whether such calls are prohibited by the TCPA without prior express consent. It is perhaps no coincidence that recognizing the FCC's failure to tackle the issue head-on and faced with a split among the circuits on the definition of autodialer, the Supreme Court granted cert, seizing the opportunity to fill the void left by the FCC's apparent intentional inaction.

The key issue in the definitional dispute involves the application of the TCPA to systems that dial from lists of stored numbers, specifically, whether the TCPA applies to systems that can "store numbers to be called" from a list, or whether the restrictions apply only to systems that "use a random or sequential number generator" when storing or producing numbers.

In 2018, the Ninth Circuit articulated a broad standard, holding that an ATDS is a device with the capacity "to store numbers to be called" and to dial such numbers automatically after the system is initiated by a person. More recently, the Second Circuit expressly adopted the Ninth Circuit's approach, holding that a system is an autodialer if it places calls from stored lists. Other appellate courts, however, have adopted a narrower definition of autodialer and have held that an ATDS must have the capacity to use a random or sequential number generator, as required by the plain language of the statute. The Eleventh Circuit came down strongly in favor of this narrow standard, holding that an ATDS must: (1) use a random or sequential number generator either to store or produce telephone numbers; and (2) dial the numbers. The Third Circuit, and most recently the Seventh Circuit, have also adopted this narrow interpretation. As the Seventh Circuit stated, to be an autodialer "a device must be capable of performing at least one of those functions [storing or producing numbers] using a random or sequential number generator."

The FCC has had ample opportunity to weigh in and resolve the definitional issue. Almost five years ago, in July 2015, the FCC issued its omnibus TCPA declaratory ruling and order and tried to fill the gap by expanding the definition of ATDS to include devices with the capability or "capacity to store or produce telephone numbers to be called, using a random or sequential number generator, and to dial such numbers," even if the device is not actually used as an ATDS. The FCC offered the following ridiculous example to explain when a device may have the capacity to autodial: "[I]t might be theoretically possible to modify a rotary-dial phone to such an extreme that it would satisfy the definition of 'autodialer,' but such a possibility is too attenuated for us to find that a rotary-dial phone has the requisite 'capacity' and therefore is an autodialer."

By resorting to comparisons with rotary phones, rather than giving real-world examples, the FCC left businesses without a practical road map for applying the law to modern communication technology.

The FCC's unclear and overbroad definition of autodialer was soundly rejected in 2018 by the U.S. Court of Appeals for the D.C. Circuit, in *ACA International v. FCC*. The court held that the FCC's definition was beyond the scope of congressional intent, leading to a potentially eye-popping sweep of the statute under which every smartphone could conceivably qualify as an ATDS.

The D.C. Circuit also found the 2015 order to be inherently contradictory; on one hand, the FCC indicated that a device must be able to generate random or sequential numbers that the device can then dial, while on the other hand also suggested that a device need only dial from a set list of numbers to constitute an ATDS.

Following the D.C. Circuit's 2018 *ACA International* decision, the FCC opened a public comment period inviting input on how the term ATDS or autodialer should be defined. A supplemental comment period followed thereafter in light of the Ninth Circuit ATDS decision in *Marks v. Crunch San Diego LLC*, which provided an expansive ATDS interpretation more aligned with the FCC's 2015 order.

A year and a half has passed since the FCC ended its supplemental comment period, but inexplicably, no further guidance has been issued. Some insight into what's happening at the FCC may be gleaned from Republican FCC Commissioner Michael O'Rielly, one of three commissioners who comprise the political majority at the FCC, who recently expressed his ongoing concern over the FCC's failure to provide a cogent working definition of autodialer, stating "the [FCC] must stop allowing legitimate callers to be unfairly punished by statutory misinterpretation and frivolous litigation."

It raises questions why the FCC's political majority is sitting idly by while the question of what constitutes an autodialer remains undefined and is subject to dispute among the courts. Caught in the crosshairs are legitimate companies looking for much-needed guidance on questions of statutory interpretation that is long overdue. The FCC has abdicated its role by failing to provide meaningful guidance under the TCPA. Where the FCC

has faltered, the Supreme Court has stepped up. Absent the Supreme Court's granting of cert, the FCC was apparently not motivated to alter the status quo, which burdens businesses, in both compliance and litigation expenses, who are seeking to comply with the TCPA.

It is shameful that corporate America has been forced to operate for so long in the dark, not knowing whether the equipment being used to place a call or send a text message will expose them to a class action. The time for the FCC to act was years ago. By failing to act, the FCC has wasted its shot and the Supreme Court is now poised to be the final arbiter of the autodialer definitional issue.

The United States Supreme Court hears oral argument on the definition of "autodialer" or "ATDS" under the TCPA: Why grammar still matters

On December 8, 2020, the U.S. Supreme Court heard oral arguments in *Facebook, Inc. v. Duguid*, a case that should provide much needed and long-awaited guidance on the definition of autodialer/ATDS under the Telephone Consumer Protection Act (TCPA). The case landed in the high court's lap following years of inaction by the Federal Communications Commission (FCC) to provide meaningful guidance on the definition of autodialer/ATDS, which created a split among federal appellate courts regarding that definition.

Enacted thirty years ago in 1991, the TCPA regulates certain telemarketing calls and was born in a different era technologically than exists today. Smart phones capable of instantaneous communication were worn on the belts of people named Kirk, Spock and McCoy, not every Tom, Jane and Mary (and their kids). Technological advances in communication technology over the past decade have triggered a proliferation of TCPA litigation, including thousands of class actions. The TCPA has become perhaps the most potent consumer protection statute of this era. At the heart of much of this litigation is the question or what constitutes an autodialer/ATDS.

The TCPA defines an ATDS as "equipment which has the capacity—(A) to store or produce telephone numbers to be called, using a random or sequential number generator; and (B) to dial such numbers." Four U.S. Courts of Appeals have adopted an expansive view of autodialer. Specifically, these Courts found that equipment will be considered an autodialer if it is capable of automatically dialing telephone numbers from a stored list, independent of whether the equipment is capable of generating random or sequential telephone numbers. By contrast, four other Circuit Courts have adopted a narrower (and more business-friendly) definition of "autodialer" by limiting it to equipment with the capacity to store or produce telephone numbers that use a random or sequential number generator.

The issue before the United States Supreme Court does not hinge on a complicated analysis of intellectual property law or complicated technical knowledge but, instead, on the unremarkable application of grammatical rules and interpretation. Simply put, the question before the Court is whether the TCPA's reference to random or sequential number generation applies to both the capacity to store telephone numbers and the capacity to produce them (the position of the First, Second, Eighth and Ninth Circuit Courts of Appeals) or whether it applies only to the capacity to produce such numbers (the position of the Third, Fifth, Seventh and Eleventh Circuit Courts of Appeal).

The impact of the Supreme Court's ruling, whichever way it rules, cannot be overstated. If the Court holds that the TCPA restricts storing numbers and calling from lists, then the TCPA will continue to impose strong restrictions on telemarketing technology and the use of dialers to place large volumes of calls. If the Court agrees with a more strict and business friendly definition of ATDS, however, then companies can avoid TCPA liability if they use autodialing systems that can simply store (but not randomly or sequentially generate) numbers and then dial them. This would significantly limit the scope of the TCPA, and would permit companies to engage in a broader range of calling practices. With any loosening of the rules on telemarketing, Congress may consider a long-overdue update to the TCPA.

ATDS circuit court standards

Broad View	Narrow View
Second Circuit *Duran v. La Boom Disco, Inc.*, 955 F.3d 279, 283 (2d Cir. 2020) (reading TCPA's ATDS definition such that "the clause requiring the use of 'a random or sequential number generator' modifies only the verb 'produce' in the statute, but not the word 'store'").	**Third Circuit** *Dominguez v. Yahoo, Inc.*, 894 F.3d 116, 121 (3d Cir. 2018) (looking to whether the device "ha[s] the present capacity to function as an autodialer by generating random or sequential telephone numbers and then dialing those numbers").
Sixth Circuit *Allan v. Pa. Higher Educ. Assistance Agency*, 968 F.3d 567, 569 (6th Cir. 2020) (holding that "the plain text of § 227, read in its entirety, makes clear that devices that dial from a stored list of numbers are subject to the autodialer ban"), petition for cert. filed, No. 19-2043 (U.S. Nov. 20, 2020).	**Seventh Circuit** *Gadelhak v. AT&T Servs., Inc.*, 950 F.3d 458, 468-69 (7th Cir. 2020) (finding device did not constitute ATDS where it did not have "capacity to generate random or sequential numbers").
Ninth Circuit *Marks v. Crunch San Diego, LLC*, 904 F.3d 1041, 1043 (9th Cir. 2018) (holding that "ATDS includes a device that stores telephone numbers to be called, whether or not those numbers have been generated by a random or sequential number generator"); *see also N.L. by Lemos v. Credit One Bank, N.A.*, 960 F.3d 1164 (9th Cir. 2020) (following *Marks*); *Duguid v. Facebook, Inc.*, 926 F.3d 1146, 1149-50 (9th Cir. 2019) (following *Marks*), *cert. granted*, No. 19-511 (July 9, 2020).	**Eleventh Circuit** *Glasser v. Hilton Grand Vacations Co.*, 948 F.3d 1301, 1306 (11th Cir. 2020) (finding that "random or sequential number generator" portion of TCPA's ATDS definition governs how numbers must be stored or produced).

* Note that while the D.C. Circuit rejected the FCC's ATDS interpretation in the July 2015 Omnibus Declaratory Ruling and Order (30 FCC Rcd. 7961 (2015)) in which the FCC looked to a device's potential ability, not just its present ability/capacity, the D.C. Circuit did not provide or suggest a new ATDS definition. *ACA Int'l v. FCC*, 885 F.3d 687, 697, 703 (D.C. Cir. 2018).

ATDS district court standards

Broad View	Narrow View
District of Massachusetts (First Circuit) *Gonzales v. HOSOPO Corp.*, 371 F. Supp. 3d 26, 34 (D. Mass. 2019) (following *Marks*).	**Eastern District of North Carolina (Fourth Circuit)** *Snow v. Gen. Elec. Co.*, No. 5:18-cv-511-FL, 2019 WL 2500407, at *6 (E.D.N.C. June 14, 2019) (following *Dominguez* and finding that ATDS is "equipment that has the capacity to store or produce numbers using a random or sequential number generator").
	Western and Northern Districts of Texas (Fifth Circuit) *Suttles v. Facebook, Inc.*, No. 1:18-cv-1004-LY, 2020 WL 2763383, at *4-6 (W.D. Tex. May 20, 2020) (declining to follow *Marks*); *Adams v. Safe Home Sec., Inc.*, No. 3:18-cv-03098-M, 2019 WL 3428776, at *3 (N.D. Tex. July 30, 2019) (finding that random or sequential generation "modifies both the numbers stored and the numbers produced" in ATDS definition).
	Western District of Missouri (Eighth Circuit) *Hand v. Beach Entm't KC, LLC*, No. 4:18-cv-00668-NKL, 2020 WL 3163672, at *6, 8 (W.D. Mo. Apr. 27, 2020) (recognizing that three other district courts in the Eighth Circuit found that "the best reading of the statute requires random or sequential number generation"). ***But see*** District of Minnesota: *Pederson v. Donald J .Trump for President, Inc.*, 465 F. Supp. 3d 929, 936 (D. Minn. 2020) (following broader interpretation of Second and Ninth Circuits).
	Western District of Oklahoma (Tenth Circuit) *Might v. Cap. One Bank (USA), N.A.*, No. CIV-18-716-R, 2019 WL 544955, at *4 (W.D. Okla. Feb. 11, 2019) (finding that equipment must have "the capacity to generate and dial random or sequential numbers").

Navigating TCPA compliance during COVID-19

As states across the US continue to operate under unprecedented stay-at-home and shelter-in-place orders with widespread restrictions of non-essential business operations in response to the COVID-19 pandemic, questions arise as to how companies may communicate with their customers, prospective customers, and employees during these strange and unsettling times. At the federal level, on March 20, 2020, the Federal Communications Commission (FCC)[1] issued a limited declaratory ruling clarifying a narrow exception from the Telephone Consumer Protection Act (TCPA) for certain COVID-19 emergency-related automated communications placed by healthcare providers or state governments. Some entities have already petitioned the FCC for an expansion of this exception for other emergency-related communications. At the state level, New York and Louisiana have increased telemarketing prohibitions for companies operating under a state of emergency.

TCPA's emergency exception as applied to COVID-19

At the federal level, the FCC has provided what should be an obvious exception from TCPA liability for certain COVID-19 emergency-related automated communications.

In a narrowly tailored declaratory ruling issued on March 20th, the FCC clarified that automated calls and texts necessitated by the COVID-19 pandemic may fall within a specific safe harbor carve-out in the TCPA for calls made for "emergency purposes." The FCC's ruling imposed specific restrictions on these calls:

(i) the caller is a hospital, healthcare provider, state or local health official, government official, or anyone acting on such organization or individual's behalf under its express direction; and (ii) the call is informational only, "made necessary" due to COVID-19, and "directly related to the imminent health or safety risk" stemming from COVID-19.[2]

Notably missing from the FCC's ruling is any exception for calls made by other businesses or industries facing emergency situations and struggling with unprecedented shut downs and disruptions. These businesses likely also have a need to contact their employees and customers through mass notifications that are not included within the scope of the FCC's ruling. See our prior alert regarding the FCC's emergency exception ruling.

On March 30, 2020, the American Bankers Association and six other financial associations filed a petition for expedited declaratory ruling, clarification, or waiver with the FCC's Consumer and Governmental Affairs Bureau (Bureau), requesting that the TCPA's emergency exception be extended to automated communications made by financial institutions in response to COVID-19.

The petition specifically references calls and texts related to customer outreach offering various services including, but not limited to, payment deferrals, fee waivers, repayment extensions, modification on mortgage or loan payments, advising customers of changes to bank operations, and informing customers of COVID-19-related programs, relief, and resources offered by the customer's banking institution. According to the petitioners, these calls and texts are "intended to protect or support the financial health or safety of consumers" and should therefore fall within the TCPA's emergency exception.[3] On April 6, 2020,

1 The FCC's Consumer and Governmental Affairs Bureau issued the declaratory ruling.
2 Mar. 20, 2020 Ruling at ¶ 7.
3 March 30, 2020 Petition at p. 5.

the Bureau issued a notice opening a public comment period that ends on May 6, 2020 (so much for any hope of an expedited ruling).

Separately, the FCC is monitoring scam communications related to the pandemic and has launched a COVID-19 Consumer Warnings and Safety Tips webpage. In its March 20th declaratory ruling, the FCC reiterated that it will vigilantly enforce prohibitions against unlawful telemarketing and fraudulent robocalls arising from COVID-19.

States of emergency and telemarketing restrictions

New York

New York enacted new telemarketing restrictions in December 2019 that are triggered in the event of a state of emergency or disaster emergency. These restrictions prohibit all "unsolicited telemarketing sales calls" during a state of emergency in New York unless the calls are placed with consent or under an established business relationship. Importantly, these restrictions apply equally to manually dialed calls as well as calls made with automated technology. New York has been operating under a state of emergency since March 7, 2020, which is expected to continue at least through September 7, 2020.

Our prior alert, which can be accessed here, provides a more in-depth overview of the current heightened telemarketing restrictions in place in New York.

Louisiana

Louisiana prohibits a "telephonic solicitor"[4] from engaging in "telephonic solicitation"[5] during a declared state of emergency, with a list of various enumerated exceptions. "Telephonic solicitation" is defined to include any voice or data communication to a residential telephone subscriber.

The list of exceptions includes, but is not limited to calls:

- made within six months in response to the called party's "express request";
- that primarily relate to an existing debt or outstanding contract performance or payment;
- made under an existing business relationship;
- made on behalf of certain non-profits; or
- made for marketing research, public opinion polling, or that constitute political activity.

Although Louisiana's governor declared a public health emergency on March 11, 2020, the state's telephone solicitation prohibitions do not yet appear to be in effect as of this writing. As explained by the Louisiana Public Service Commission (LPSC), the state's Office of Homeland Security and Emergency Preparedness requires the LPSC to report on additional telephonic solicitation prohibitions during a state of emergency. According to the LPSC's website, the LPSC has not yet been required to report on any additional restrictions, and "no additional telephonic solicitation prohibitions are necessary at this time."

Even if Louisiana's heightened ban on telephone solicitation is not fully in force yet, companies conducting business in Louisiana should take into account other reputational and consumer-facing considerations when determining how to communicate with customers and prospective customers during this time.

Conclusion

COVID-19 has undoubtedly added further complications to navigating TCPA compliance as the country experiences unprecedented restrictions and closures. At the federal level, the FCC has applied a narrow exception for limited automated communications in relation to COVID-19, but questions remain as to whether the FCC's interpretation of the exception will be expanded in light of a recent petition by the American Bankers Association and other financial associations. Telemarketing restrictions also vary by state, adding to the growing list of COVID-19-related compliance considerations for industries communicating with their customers, prospective customers, and employees during the outbreak.

The FCC confirmed that callers may lawfully make automated calls and send automated text messages to wireless telephone numbers when such calls are necessary to protect the health and safety of citizens pursuant to the TCPA's "emergency purposes" exception.

4 The Louisiana statute defines a "telephonic solicitor" as: "any natural person, firm, organization, partnership, association, or corporation, or a subsidiary or affiliate thereof, doing business in this state, who makes or causes to be made a telephonic solicitation, including but not limited to any communication made by use of automated dialing or recorded message devices." La. Stat. Ann. § 45:844.31(B)(3).

5 The Louisiana statute defines "telephonic solicitation" as "any voice or data communication made by a telephonic solicitor to a residential telephonic subscriber for any of the following purposes:
(i) Encouraging a sale or rental of or investment in property, consumer goods, or services.
(ii) Encouraging an extension of credit for property, consumer goods, or services.
(iii) Obtaining information that will or may be used for the direct solicitation of a sale or rental of or investment in property, consumer goods, or services or an extension of credit for such purposes.
(iv) Soliciting of a contribution to a charitable organization."
Id. at § 45:844.31(B)(2)(a). There is an explicit exemption for the American Red Cross and certain Louisiana-based community blood centers with IRC 501(c)(3) non-profit status.
Id. at § 45:844.31(B)(2)(b).

FCC offers new guidance on TCPA emergency exception as applied to COVID-19, clarifies status of Solicited Fax Rule

As the US continues to experience mass closures, a national state of emergency and unprecedented restrictions in response to the COVID-19 outbreak, the Federal Communications Commission (FCC or Commission) has recently released a rather unremarkable declaratory ruling—providing what should be an obvious exception for certain limited COVID-19 emergency related automated communications from the Telephone Consumer Protection Act (TCPA)—and an order confirming what we already knew, namely that the now-defunct Solicited Fax Rule, which was struck down by a federal appellate court three years ago, is, indeed, dead.

With myriad other pressing issues pending before it, including the definition of autodialer (or ATDS), it is disappointing that the FCC has elected to focus its attention and resources on housekeeping matters and clearing out a backlog of petitions relating to the Solicited Fax Rule that it should have addressed years ago. The FCC needs to give meaningful and long overdue guidance to the industries and broad industry segments that are most affected by the TCPA, which the declaratory ruling and order unfortunately do not provide.

FCC declaratory ruling applies limited emergency exception to COVID-19

In its March 20, 2020 declaratory ruling, the FCC[1] clarified that a narrow group of automated communications arising from the COVID-19 outbreak fall within the TCPA's emergency exception, which exempts automated calls that are made for "emergency purposes."[2] FCC rules define "emergency purposes" as calls that are "necessary in any situation affecting the health and safety of consumers."[3] The FCC has interpreted the emergency exception narrowly for situations giving rise to significant public health and safety risks where automated communications could allow for more efficient information-sharing regarding "potentially hazardous [public] conditions."[4]

In order for COVID-19 related automated communications to qualify for the TCPA's emergency exception: (i) the caller must be a hospital, healthcare provider, state or local health official, government official, or anyone acting on such organization or individual's behalf under its express direction; and (ii) the call must be informational only, "made necessary" due to COVID-19, and "directly related to the imminent health or safety risk" stemming from COVID-19.[5]

To illustrate COVID-19's application to the emergency exception, the ruling provides non-exhaustive examples of automated calls made for an "emergency purpose," such as those placed by a government official informing individuals regarding shelter-in-place requirements, quarantines, or school closures arising from the outbreak. Conversely, the FCC clarified that advertising and telemarketing calls, such as those for commercial grocery delivery services, health insurance, and cleaning services as well as debt collection calls do not fall within the exception.

Notably, the FCC's ruling does not address calls made by other businesses or industries that may also be facing emergency situations as a result of COVID-19.

Despite providing narrow relief for certain callers under limited COVID-19 circumstances, the FCC reiterated that it will continue to vigilantly enforce prohibitions against unlawful telemarketing and fraudulent robocalls arising from COVID-19.

1 The Consumer and Governmental Affairs Bureau within the FCC issued the March 20, 2020 declaratory ruling.
2 47 U.S.C. § 227(b)(1)(A)-(B).
3 47 C.F.R. § 64.1200(f)(4).
4 *See* 7 FCC Rcd. 8752, 8788 (1992).
5 Mar. 20, 2020 Ruling at ¶ 7.

FCC order affirms elimination of the Solicited Fax Rule

Aside from COVID-19, the FCC has affirmed the Consumer and Governmental Affairs Bureau's elimination of the Solicited Fax Rule following a decision in 2017 by the D.C. Circuit that the FCC lacked the authority to adopt the rule in the first place. The Solicited Fax Rule, adopted by the FCC in 2006, required that opt-out notices be provided on solicited facsimile advertisements sent at recipients' invitation or with their permission.

The US Court of Appeals for the D.C. Circuit struck down the Solicited Fax Rule in 2017, finding that the FCC was not authorized under the TCPA to adopt the rule.[6] Specifically, the D.C. Circuit found that the TCPA only requires opt-out notices on *unsolicited* facsimile advertisements, and therefore "Congress drew a line . . . between unsolicited fax advertisements and solicited fax advertisements."[7] According to the D.C. Circuit, the FCC impermissibly crossed that line when it attempted to expand opt-out notice requirements to even solicited faxes.

Following the D.C. Circuit's decision, the FCC's Consumer and Governmental Affairs Bureau eliminated the Solicited Fax Rule in 2018. Bureau rulings may be appealed to the full Commission by filing an application for review following the ruling, which is what a group of TCPA plaintiffs did in December 2018, arguing in part that the D.C. Circuit's decision did not constitute a non-discretionary mandate to eliminate the rule. Other petitions have since been filed.

The FCC has provided what should be an obvious exception for certain COVID-19 emergency related automated calls and texts. In addition, the FCC has unsurprisingly affirmed the elimination of its Solicited Fax Rule after a prior finding by the D.C. Circuit that it lacked authority in adopting the rule back in 2006. Perhaps we will soon see further action by the FCC on issues of paramount importance to the business community like a coherent definition of what constitutes an autodialer (or ATDS).

On March 17, 2020, the FCC found that the Bureau's elimination of the Solicited Fax Rule was "necessary and appropriate," thereby (rather unremarkably) affirming the Bureau's decision.[8] The FCC clarified that allowing the Solicited Fax Rule to remain on the books would "serve[] no public interest" and would rather "create unnecessary confusion and consternation."[9] Because the D.C. Circuit found the Solicited Fax Rule to be an unlawful exercise of the FCC's authority under the TCPA, the FCC held that the Bureau acted properly in eliminating the rule. The FCC has thus recognized, three years after the D.C. Circuit's ruling, that it is obliged to comply with the D.C. Circuit's mandate striking down the Solicited Fax Rule.

Conclusion

The FCC has provided what should be an obvious exception for certain COVID-19 emergency related automated calls and texts. In addition, the FCC has unsurprisingly affirmed the elimination of its Solicited Fax Rule after a prior finding by the D.C. Circuit that it lacked authority in adopting the rule back in 2006. Perhaps we will soon see further action by the FCC on issues of paramount importance to the business community like a coherent definition of what constitutes an autodialer (or ATDS).

6 *See Bais Yaakov of Spring Valley v. FCC*, 852 F.3d 1078, 1083 (D.C. Cir. 2017).
7 *Id.* at 1082.
8 Mar. 17, 2020 Order at ¶ 11.
9 *Id.*

TCPA best practices—top five do-not-call list (DNC) compliance tips

Meeting the requirements of federal and state Do-Not-Call laws (DNC) is a key component of telemarketing compliance. The National Do-Not-Call Registry is a national database that permits consumers to register their telephone numbers to prevent unsolicited calls from telemarketers and others. The DNC rules generally prohibit companies from placing telemarketing calls to consumers whose numbers are listed in the National DNC Registry, subject to certain exceptions. In addition, consumers may elect to be added to a company's internal, company-specific DNC list.

How do companies effectively monitor the National DNC Registry to ensure compliance and avoid litigation under the Telephone Consumer Protection Act (TCPA) and related state laws? This legal alert discusses five key tips for implementing and maintaining an effective DNC compliance policy.

1. DNC Compliance Requires Checking *Both* Federal and State Registries

Federal regulations require that companies engaged in telemarketing scrub their calling lists and databases to avoid calling numbers listed on the National DNC Registry. While many states have adopted the National DNC Registry as their official statewide registry, 12 states, including Colorado, Florida, Indiana, Louisiana, Massachusetts, Mississippi, Missouri, Oklahoma, Pennsylvania, Tennessee, Texas and Wyoming continue to implement separate state registries. Residents in these states may register their telephone numbers on their state's DNC list, and companies must abide by state DNC rules in addition to federal rules. A handful of states permit a consumer to file a private lawsuit for state law violations of the DNC rules, similar to TCPA litigation under federal law.

As a result, companies seeking to implement an effective DNC compliance policy must ensure that their employees and third-party vendors check their call lists against all applicable DNC databases before placing calls to consumers.

2. Put It In Writing: A Company-Specific DNC List Requires a DNC Compliance Policy, Implementation and Tracking of Opt-Outs

Under the TCPA, companies may not make telemarketing calls to consumers who have requested not to receive calls made by or on behalf of specific companies. Companies must, therefore, maintain company-specific DNC lists. Companies may not make telemarketing calls (or have third-parties make calls on their behalf) unless, and until, they have implemented procedures to maintain their internal DNC list. Stated differently, companies must honor requests to stop calling, and maintain procedures for doing so.

TCPA rules articulate minimum standards for company-specific DNC compliance, including:

- A written policy. Companies or third-party vendors engaged in telemarketing should have a written policy, available on demand, for maintaining a company-specific DNC list;
- Recording DNC requests. If a company making a call for telemarketing purposes (or on whose behalf the call is made) receives a request from a consumer not to receive calls from that company, the company should record the request and place the subscriber's name, if provided, and telephone number on the company-specific DNC list;
- Honor DNC requests promptly. The consumer's DNC request must be honored within a reasonable time, but no later than thirty (30) days from the date of the request;
- Affiliated person or entities. The consumer's DNC request applies to affiliated entities, if the consumer reasonably would expect them to be included, given the identification of the caller and the product or service being advertised;

- Training of personnel. Personnel participating in telemarketing must be informed and trained in the existence and use of the company-specific DNC list;
- Confidentiality. A consumer's DNC request may not be shared with any third-party, other than the entity on whose behalf a telemarketing call is made or its affiliate, without the consumer's prior express consent; and
- Maintenance of DNC Lists. Under federal law, a company-specific DNC request must be honored for five years from the time the request is made (state laws vary).[1]

3. Know the Limits of the Established Business Relationship Exception

Federal DNC regulations provide an exception for calls to current consumers or those who have recently requested information from a company. Companies may call a consumer listed on the National DNC Registry when, the seller or telemarketer "can demonstrate that the seller has an *established business relationship* (EBR) with such person, and that person has not stated he or she does not wish to receive outbound telephone calls."[2] Under DNC rules, a company has an established business relationship with a consumer if: (a) the consumer has entered into a transaction with the seller within the previous 18 months, or (b) the consumer inquired about the seller's goods/services within the previous three months.

State DNC rules can vary, however, on the scope of the EBR exception. Although many state laws are harmonized with federal laws, certain states have imposed EBR rules that are more restrictive than the federal rules. There are generally two areas of divergence between the state and federal EBR rules. First, some states implement an EBR exception that extends for a shorter amount of time than the 18-month period provided under the federal rule (generally 12 months). Second, some states implement a more restrictive EBR definition that does not permit communication based solely on a consumer inquiry.

4. Maintain DNC Compliance Policies and Procedures to Avoid Litigation Risks

DNC violations can create significant litigation risk under the TCPA. Class action lawsuits are common, and with statutory damages of $500 per call (and up to $1,500 per call for willful violations), exposure can escalate rapidly into the millions of dollars. In one notable (and extreme) series of cases, courts have entered judgments for more than $300 million against a company for systemic DNC compliance failures. The wave of litigation is likely to continue.

One key mitigation strategy for DNC is to qualify for the "safe harbor" provision for bona fide errors. FCC rules permit companies to avoid liability for inadvertent calls to numbers on the National DNC Registry, provided each company has certain procedures in place. In order to invoke the TCPA's safe harbor provision, companies must demonstrate that, as part of the seller's or telemarketer's routine business practice, they have:

- Established and implemented written procedures;
- Conducted employee training;
- Maintained and recorded a list of telephone numbers the seller or charitable organization may not contact;
- Established a process to prevent telemarketing to any telephone number on the National DNC Registry;
- Checked call lists against a version of the National DNC Registry obtained within the past month;
- Maintained records documenting this process;
- Monitored and enforced compliance with the procedures; and
- Purchased the National DNC Registry without participating in an arrangement to share costs of access.[3]

This safe harbor provision, although limited to calls made as a result of *bona fide* error, underscores the need for companies to implement a comprehensive DNC compliance policy.

Adhering to the requirements of both state and federal Do-Not-Call laws (DNC) is a crucial component of TCPA compliance. In implementing and maintaining an effective DNC compliance policy, it is important to keep in mind that DNC compliance is in addition to autodialer compliance, which separately requires companies to obtain the requisite levels of consent prior to autodialing or sending prerecorded messages or blast texting campaigns.

1 47 C.F.R. § 64.1200(d).
2 16 C.F.R. § 310.4(b)(iii)(B)(2).
3 47 C.F.R. § 64.1200(c)(2).

5. Keep it Straight: DNC Compliance is in *Addition* to TCPA Autodialer Compliance

One common misconception is that compliance with DNC rules alone is sufficient to avoid TCPA liability. The DNC compliance is only half the battle. The TCPA requires that companies obtain consent – written or express – prior to autodialing, sending prerecorded messages, or blast texting. These requirements are separate and distinct from, and in addition to, DNC requirements.

For instance, companies may not make autodialed telemarketing calls to consumers, even after checking the National DNC Registry, unless the consumer has provided signed written consent to receive autodialed calls. Similarly, companies calling consumers under the EBR exception (consumers with whom the company has recently done business) are permitted to make *manual* calls under DNC rules, but cannot make *autodialed* calls without prior express written consent. TCPA regulation is a multilayered set of requirements; therefore, an effective compliance program must consider both DNC and autodialer rules.

Conclusion

DNC compliance is an important part of any telephone marketing campaign. With the ongoing wave of lawsuits alleging DNC violations, companies will need to maintain a focus on its compliance efforts to mitigate their potential risks under the TCPA.

Four common risks in text message programs . . . and how to avoid them

Although the Telephone Consumer Protection Act (TCPA) may be most commonly known for its prohibitions on robocalls, text messages also fall within the TCPA's broad scope. Given the outsize risk of class action TCPA litigation arising from text messaging, it is important to understand the requirements for maintaining a texting program that is compliant with the TCPA, Federal Communications Commission (FCC) regulations, and industry standards. This legal alert discusses four common risks that companies can face when using text messaging to communicate with their customers, and offers commentary on these challenging issues.

Risk One: Failing to Employ Sufficient Opt-In Mechanisms

The TCPA requires that companies obtain the appropriate level of consent for automated communications, including text messages.[1] For texts, best practices include: (1) requiring consumers to provide consent by affirmatively opting-in to receive text messages; and (2) using a "double opt-in" procedure if the consumer initially agrees to receive text messages in a manner other than via a text from his or her phone, such as by completing an online form or verbally agreeing to join the campaign. These practices are consistent with industry compliance standards.

Scenario One: A utility company sends one text to a customer as a kickoff to its text campaign by notifying the customer that he is subscribed to the company's outage alerts. This scenario is modeled off of *Grant v. Commonwealth Edison Co.*, Case No. 1:13-cv-08310, in the Northern District of Illinois. Although the company argued that the customer provided his "prior express consent" to receive the text regarding outage alerts because it was part of an informational safety program, the company ultimately agreed to establish a multimillion-dollar settlement fund.

Scenario Two: A store clerk asks a customer if she would like to enroll in the company's rewards program. The customer verbally agrees and receives a text thanking her for enrolling in the program and prompting her to download the company's app. This scenario is based off of the class action case, *San Pedro-Salcedo v. Haagen-Dazs Shoppe Co.*, Case No. 5:17-cv-03504-EJD, currently pending in the Northern District of California. The court denied the company's motion to dismiss in holding that the text, by prompting the customer to download the app, arguably advertised the app. A motion to certify the class was filed and a hearing was held in June 2019.[2]

Eversheds Sutherland Commentary: Consistent with industry standards, it is important to employ opt-in or "double opt-in" to obtain consent from consumers who enroll in text campaigns.

> For companies that communicate with customers and potential customers through text messaging, text campaigns can present ongoing risks of liability. Understanding and avoiding the common risks associated with texting programs is a critical component of mitigating exposure under the TCPA.

Risk Two: Relying Solely on Indirect Consent

Perhaps a more complicated and not so readily apparent issue involves consent that has been conveyed by a third party rather than by the consumer directly. The FCC has held that a consumer's consent can be "obtained through and conveyed by an intermediary," but the intermediary cannot consent on the consumer's behalf.[3]

1 *Compare* 47 C.F.R. § 64.1200(a)(1), *with* 47 C.F.R. § 64.1200(a)(2).
2 Update: The Court, without hearing oral argument, denied the plaintiff's motion to certify the class in December 2019. The parties have since settled.
3 *See* 29 F.C.C. Rcd. 3442, 3444, 3447 ¶¶ 6-7, 14 (2014).

Scenario One: In seeking medical treatment, a patient provides his girlfriend's cell phone number during the intake process. The patient was allowed to use his girlfriend's cell phone for emergency purposes with his girlfriend's permission and may have additionally used her cell phone number in other circumstances as well. The girlfriend subsequently received autodialed calls to collect money owed by the patient for his medical treatment. This scenario is modeled off of the case, *Jackson v. PMAB, LLC*, 2017 WL 4316096 (D. N.J. Sept. 28, 2017). The court in *Jackson* denied the plaintiff's motion for summary judgment by holding that a genuine issue of material fact existed as to whether the girlfriend, as the call recipient, gave her express consent to the patient to provide her cell phone number for communications related to his medical treatment. Although *Jackson* suggests that this inquiry is based on the particular facts at issue in each case, companies risk TCPA liability when they fail to obtain the direct consent of the call or text recipient.

Scenario Two: A group messaging company requires only that the individual who creates the group message consents to receive future texts. Modeled after a 2014 Order, the FCC held that the group messaging platform could be liable under the TCPA if its users who create the group messages do not receive the prior express consent of the other group members. The FCC encouraged text platforms to "ensure that [text message] group organizers do in fact obtain the requisite consent."[4]

Eversheds Sutherland Commentary: Appreciate the distinctions between relaying the consent of the text message recipient and providing consent on behalf of the text message recipient. This is a case-by-case analysis and likely one that may not be readily inferred based on the parties' relationship alone. Furthermore, complying with opt-in requirements, and providing easy-to-follow instructions to unsubscribe from text messages, are important considerations to limit exposure in complex situations such as these.

Risk Three: Misunderstanding the Emergency Exception

The TCPA provides an express exception from the consent requirement for communications that are made for "emergency purposes."[5] FCC regulations define "emergency purposes" as "situation[s] affecting the health and safety of consumers."[6]

Scenario: A parent provides his or her cell phone number to a school as a contact. The school does not disclose the types of messages the parent may receive, and subsequently sends the parent automated texts regarding a weather-related closure, an upcoming parent-teacher conference, and a non-school, community event taking place at the school. In a 2016 Order, the FCC clarified that schools may rely on the TCPA's emergency exception to send automated texts for limited purposes regarding weather-related closures, threats or health risks, and unexcused absences.[7] Therefore, according to the FCC, the first text would fall within the emergency exception. Importantly, the FCC held that automated non-emergency, school-related texts still require the recipient's prior express consent, which is generally satisfied when students or parents provide their phone numbers as a school contact. In the FCC's view, texts regarding parent-teacher conferences are closely related to the school's educational mission, and consent to receive such messages is likely satisfied by virtue of the parent providing his or her number to the school. On the other hand, the FCC found that texts regarding non-school events are not closely related to the school, and therefore consent is not similarly satisfied when the parent provides his or her number to the school.

Eversheds Sutherland Commentary: While the FCC has recognized the emergency exception in limited circumstances, a text campaign can ensure compliance by adhering to federal rules and industry standards even where such an exception might arguably apply.

Risk Four: Giving Mixed Signals Regarding Program Costs

FCC regulations require that a consumer's prior express written consent be part of a "clear and conspicuous disclosure . . . ."[8] Companies may face this risk if their disclosures lack clear language or otherwise do not comply with industry guidance.

Scenario: A company's call-to-action program, which encourages consumers to text a keyword or phrase to join the program or to receive a discount or promotion code, does not charge consumers to join or be eligible to receive the promotion. The company's disclosure tells consumers that it is free to participate. Industry guidance requires that such text campaigns disclose that message and data rates may apply. Therefore, companies cannot misinform consumers about the costs associated with their programs by implying that they are free even though consumers may still incur charges associated with standard message and data rates.

4 29 F.C.C. Rcd. 3442, 3447 ¶ 13 (2014).
5 47 U.S.C. § 227(b)(1)(A).
6 47 C.F.R. § 64.1200(f)(4).
7 31 F.C.C. Rcd. 9054, 9061 ¶ 17 (2016).
8 47 C.F.R. § 64.1200(f)(8)(i).

Eversheds Sutherland Commentary: Use of confusing or misleading language in marketing disclosures encompasses a broader risk if companies do not adhere to industry guidance on how costs and other aspects of the campaign are communicated to consumers.

Conclusion

While text campaigns can be an efficient and cost-effective means of advertising and growing a customer base, they present ongoing risks of liability. Avoiding the common risks associated with texting programs is one critical component of mitigating exposure and potential liability under the TCPA. For companies that communicate through automated calls and text messages, it is important to have a robust compliance program and to understand what the business intends to communicate to the call and text recipients. There is often a gray area between a message that does not violate the TCPA and one that does violate the TCPA. Understanding and addressing the distinctions, including those described above, can mean the difference in avoiding costly litigation, including class action complaints.

Eversheds Sutherland Observation: Common risks associated with text campaigns include failing to employ sufficient opt-in mechanisms to receive texts, relying solely on recipients' indirect consent, misunderstanding the FCC's emergency exception from the consent requirement, and using confusing or misleading language in marketing disclosures.

TCPA so far shows distinct lack of clarity

The Telephone Consumer Protection Act (TCPA) is perhaps the most significant consumer protection act of our era. Enacted in 1991, when calling technology and mobile phones were in their infancy, the TCPA restricts how companies may communicate with their customers and prospective customers.

For telemarketing purposes, the TCPA requires that cell phone call (or text) recipients provide prior written consent. For non-marketing calls, prior express consent is required.

In today's technology-driven era, thousands, if not tens of thousands, of calls/texts may be transmitted over a very short period. With penalties for violating the TCPA at $500 per violation (trebled to $1,500 if the conduct is deemed willful), with no cap on liability, TCPA damages can easily climb into the millions.

Companies need to keep an eye on four TCPA issues in 2020:

1. the definition of autodialer;
2. implementation of the reassigned cellular number database;
3. the impact of the Pallone-Thune TRACED Act; and
4. whether the U.S. Supreme Court will continue to afford the FCC deference in TCPA cases.

What Is an Autodialer? Still Seeking Clarity

Courts and businesses continue to struggle with the foundational TCPA question of what constitutes an automatic telephone dialing system (ATDS). In late January 2020, the U.S. Court of Appeals for the Eleventh Circuit held that to be an ATDS, equipment must:

1. use a random or sequential number generator to store or produce telephone numbers; and
2. dial the numbers.

Thus, equipment used to make calls to a pre-selected list of recipients, whose numbers were not produced or stored using a random or sequential generator, is not an ATDS within the meaning of the statute *(Glasser v. Hilton Grand Vacations Co. LLC)*. The court rejected the plaintiffs' argument that the statutory phrase "using a random or sequential number generator" modifies only "produce," and not "store," such that equipment that simply stores and dials telephone numbers could be an ATDS.

More recently, the Seventh Circuit joined the Eleventh Circuit in holding that an ATDS within the meaning of the TCPA is equipment that uses a random or sequential number generator (*Gadelhak v. AT&T Srvcs. Inc.*).

Implementation of Reassigned Cellular Number Database

The FCC has authorized the creation of a reassigned cellular number database, the purpose of which will be to determine whether consumers have been reassigned a cellular telephone number. The FCC also created a potential safe harbor from TCPA liability.

Companies that use the reassigned cellular number database will, theoretically, be able to determine if cellular numbers on their calling lists have been disconnected and made eligible for reassignment. Companies can then purge these numbers from their call lists, thereby decreasing the number of errant calls to consumers who are not the intended recipient.

To further encourage the use of the database, the FCC is providing callers with a safe harbor from liability for calls made to reassigned cellular numbers due to a database error.

With the wave of TCPA litigation expected to continue, developments in these key areas will shape the TCPA landscape. Plaintiffs' lawyers will continue to target many different industries, and a strong TCPA compliance program is essential to help businesses of all kinds avoid TCPA lawsuits and potential exposure.

Impact of the Pallone-Thune TRACED Act

In a renewed effort to combat robocalls, Congress enacted the Pallone-Thune TRACED Act. A crucial element of the TRACED Act is assigning new responsibilities and obligations to phone-service providers to identify calls correctly and shield their customers from unwanted calls.

The act will require phone-service providers to implement a new caller-ID authentication program that will enable providers to block unwanted calls. Providers must implement the caller-ID authentication program at no additional cost to the customer. The authentication program is aimed at cutting down on the practice of "spoofing," where scammers trick consumers into thinking a call is coming from a specific area code or a legitimate place of business.

The act also gives the FCC new tools to increase its enforcement actions, including a longer statute of limitations and assessment of higher fines and penalties for offenders.

The U.S. Supreme Court Weighs in on TCPA Issues

In 2019, the Supreme Court was asked to determine whether federal courts are bound by FCC guidancein TCPA cases. The question on appeal in *PDR Network LLC v. Carlton & Harris Chiropractic Inc.* was whether the Hobbs Act—which grants exclusive jurisdiction to federal appellate courts to set aside, suspend, or rule on the validity of certain federal agency guidance—requires district courts to defer to FCC rulings and orders interpreting the TCPA.

The Supreme Court vacated the Fourth Circuit's decision and remanded. It held that two preliminary questions needed to be addressed before the court could consider whether district courts are bound by FCC interpretations under the Hobbs Act:

1. whether the 2006 FCC order at issue is a legislative rule that has the force of law or whether it is an interpretive rule that advises on the agency's construction of the law but does not have the effect of law; and
2. whether PDR Network had a prior and adequate opportunity to seek judicial review of the order under the Hobbs Act petition.

In remanding the case, the Supreme Court punted on the core question presented; i.e., whether district courts in private litigation are required to defer to the FCC under the Hobbs Act, or whether courts have authority to interpret and apply unambiguous statutory provisions that conflict with FCC rules.

The Fourth Circuit's ruling on remand in 2020 may set this up for further high court review, and the question is also expected to arise in other cases.

The Supreme Court may weigh in on the definition of ATDS if it grants certiorari in *Duguid v. Facebook Inc.* One of the questions on appeal is whether the definition of an ATDS encompasses any device that can "store" and "automatically dial" telephone numbers, even if the device does not use a random or sequential number generator.

In *Facebook*, the Ninth Circuit defined ATDS broadly to include any device that can "store" and "automatically dial" telephone numbers, even if the device does not use a random or sequential number generator.

With the wave of TCPA litigation expected to continue, developments in these key areas will shape the TCPA landscape. Plaintiffs' lawyers will continue to target many different industries, and a strong TCPA compliance program is essential to help businesses of all kinds avoid TCPA lawsuits and potential exposure.

Modern day bank robbery: Banks face increasing TCPA class action liability

Willie Sutton is alleged to have said *"I rob banks because that's where the money is."* The same can be said for plaintiff's lawyers who over the past several years have filed an increasing number of TCPA class actions against banks and other financial institutions.

Over the past several years banks and other financial institutions have been targeted in numerous putative class actions alleging violations of the TCPA that resulted in multimillion-dollar judgments and settlements. The high value of these settlements illustrates how automated communications can pose significant litigation risks that can be mitigated only through an understanding of the requirements of TCPA and a robust focus on compliance. Banks and other financial institutions often communicate with existing and prospective customers through automated communications for purposes of marketing, customer servicing, and collections—making companies operating in the financial sector frequent targets of claims brought under the Telephone Consumer Protection Act (TCPA).

TCPA Background

Enacted in 1991 to protect consumers from receiving unsolicited telemarketing calls and faxes (and more recently text messages), the TCPA regulates and restricts the manner in which a business may advertise its products and services to consumers or otherwise communicate with its customers. Specifically, the TCPA prohibits the use of an "automated telephone dialing system" or an "artificial or prerecorded voice" to make calls to cell phones without obtaining the recipient's consent. Certain restrictions apply to telemarketing and non-telemarketing calls alike, including debt collection or informational calls. These same rules apply to banks and other financial institutions.

Class action risk under the TCPA can be considerable. Because the TCPA provides for statutory damages of $500 per violation (and up to $1,500 per willful violation) with no maximum cap on recovery, potential exposure in a TCPA class action can quickly escalate into the millions.

Federal Communications Commission (FCC) regulations interpreting and implementing the TCPA require consent for most automated telemarketing communications. Specifically, prior express written consent is required for autodialed or prerecorded telemarketing calls or texts to cell phones. These requirements also apply to prerecorded telemarketing calls to landlines, and there is no exception for calls to customers with whom the company has an established business relationship. For purposes of the regulations, the term "prior express written consent" means an agreement in writing, with a signature in some form that clearly authorizes the seller to make telemarketing calls or texts using an autodialer or a prerecorded voice.

Financial institutions face potential litigation exposure under the TCPA through conduct such as communication through phone, text, or fax, using an automatic telephone dialing system or through the use of independent or semi-independent agents that participate in such automated communications. Organizations should be aware of various issues arising under the TCPA involving vicarious liability, the definition of "telemarketing," as well as federal, state, and company-specific do not call restrictions, the FCC's reassigned number database, and the narrow health care exemption recognized by the FCC.

TCPA Class Actions Continue to Target Banks and Other Financial Institutions

The TCPA continues to raise litigation and compliance challenges across the financial services industry, with scores of lawsuits being filed against banks and other financial institutions each year. These class action lawsuits have challenged both marketing calls and/or non-marketing calls, including servicing and collection calls, and have resulted in several high-dollar settlements. Just over the past year, Wells Fargo settled TCPA class actions for over $17 million. Multimillion-dollar TCPA class action settlements have also been reported recently by, among others, HSBC and Compass Bank. In the Wells Fargo case the complaint alleged that the bank violated the TCPA by improperly sending unsolicited prerecorded messages to cell phones about mortgages, home equity loans, credit card accounts, auto loans, student loans, and fraud alerts. Common, but dangerous, practices for bank communications.

FCC Guidance for the Banking Industry

The FCC has issued specific guidance clarifying that banks and other financial institutions may make automated calls and texts to their customers concerning data breaches without violating the TCPA. Specifically, the FCC created an exemption for calls intended to prevent fraudulent transactions or identity theft, including data security breaches, provided that the messages do not include marketing, advertising, or debt collection, and that each message includes information regarding how to opt out of future messages. Financial institutions are limited to no more than three calls over a three-day period. According to the FCC, these types of calls are intended to address exigent circumstances in which a quick, timely communication with a consumer could prevent considerable consumer harm or mitigate the extent of such harm. The FCC also exempted from the consent requirement calls regarding money transfers, including notifying the recipient of steps to be taken to receive the transferred funds.

Conclusion

The TCPA challenges facing the banking and financial services sector are expected to continue as companies seek to protect themselves from continuing risk of litigation. A strong TCPA compliance program is essential to help understand the type of communications permissible under the Act and to minimize potential liability.

Financial institutions face potential litigation exposure under the TCPA through conduct such as communication through phone, text, or fax, using an automatic telephone dialing system or through the use of independent or semi-independent agents that participate in such automated communications. Organizations should be aware of various issues arising under the TCPA involving vicarious liability, the definition of "telemarketing," as well as federal, state, and company-specific do not call restrictions, the FCC's reassigned number database, and the narrow health care exemption recognized by the FCC.

NY's Nuisance Call Act goes into effect; NY state of emergency prompts further marketing call restrictions

New York's Nuisance Call Act (NYNC Act), signed into law in December 2019 and effective as of March 1, 2020, amends New York's telemarketing law (specifically, N.Y. Gen. Bus. Law § 399-z) by requiring live voice outbound telemarketers to inform consumers that they may be added to the seller's internal do-not-call (DNC) list (remember, there are three DNC lists: federal, state and company-specific). New York's telemarketing laws generally apply to calls made to customers located within the state. Under the new provision of Section 399-z of the New York General Business Law, if a consumer chooses to be placed on the company-specific DNC list, the telemarketer must immediately end the call and add the number to the company's internal DNC list to prevent future calls. Prior to the NYNC Act, this requirement applied only to pre-recorded voice calls.

In addition, the NYNC Act restricts the sharing of customer data by requiring telemarketers and sellers to obtain a consumer's "express agreement," in writing or electronic format, before transmitting, sharing, or otherwise making available any customer's contact information, including name, telephone number, or email address, unless such disclosure is required by law or under a lawful subpoena or court order.

The NYNC Act retains a safe harbor exemption for companies that have obtained a version of the national DNC list from the Federal Trade Commission no more than 31 days before the call at issue is made and that have implemented comprehensive and documented (written) DNC policies and procedures.

The NYNC Act also retains notice and due process provisions that allow for an administrative hearing before an adjudication of liability. The penalty for violations of New York's telemarketing restrictions under Section 399-z of the New York General Business Law cannot exceed $11,000 per violation. New York does not provide for a private right of action but does not "restrict any right which any person may have under any other statute or at common law." Stated otherwise, an aggrieved called party may still sue under the Telephone Consumer Protection Act (TCPA).

Further telemarketing restrictions separate from those added by the NYNC Act were also signed into law in New York in December 2019. Those restrictions are triggered in the event of a state of emergency or disaster emergency in the state, and should be on companies' radar because on Saturday, March 7, 2020, New York Governor Andrew Cuomo declared a state of emergency due to the spread of the coronavirus in the state.

As more fully discussed below, the new emergency restrictions change the permissible telemarketing landscape in New York in times of a state of emergency by prohibiting all unsolicited telemarketing sales calls—whether dialed manually, dialed by an automatic telephone dialing system (ATDS) or aided by other technology—unless they are made with consent or under an established business relationship. This is different from the traditional, non-state of emergency rules, where a caller need only have consent to place auto-dialed telemarketing sales calls.

Specifically, as a result of the declaration by Governor Cuomo, placing unsolicited telemarketing sales calls is restricted until the state of emergency is lifted. The restrictions added to New York's telemarketing laws in December 2019 amend two separate statutory sections: Section 399-z (discussed above as also having been separately amended under

Impact: So long as New York is under a state of emergency, unsolicited telemarketing sales calls, whether manually or auto-dialed, may not be made unless the call recipient has provided consent or there is an established business relationship between the caller and call recipient, and consent has not been withdrawn. Once the state of emergency is lifted, New York's traditional telemarketing laws should apply, requiring consent (in the specific form provided under the statute) only for auto-dialed telemarketing sales calls. It is important to remember that additional opt-out requirements and restrictions on sharing of customer information have also recently been added to New York's telemarketing laws and apply regardless of any state of emergency.

the NYNC Act) and Section 399-pp of the New York General Business Law. The new restrictions are the same under both sections, namely that a telemarketer cannot "knowingly make an unsolicited telemarketing sales call to any person in a county, city, town or village under a declared state of emergency or disaster emergency . . . ." The term "unsolicited telemarketing sales calls" is defined under Section 399-z as any telemarketing sales calls (which include calls placed by a telemarketer or by an outbound calling technology) except for those made:

(i) In response to an express written or verbal request by the customer; or

(ii) In connection with an established business relationship, which has not been terminated by either party, unless such customer has stated to the telemarketer that such customer no longer wishes to receive the telemarketing sales calls of such telemarketer.

Absent a state of emergency, New York's telemarketing laws require that telemarketers or sellers placing technology-aided telemarketing sales calls—or in other words, calls placed by an ATDS or technology that delivers a pre-recorded message to the recipient—first receive the recipient's consent in writing through an express agreement. *See* N.Y. Gen. Bus. Law § 399-z(6). New York's telemarketing laws are consistent with the TCPA in this respect in that technology-aided calls may be made only with the consent of the called party, but manually dialed calls may be made without such consent (assuming compliance with the opt-out requirements added under the NYNC Act).

There is one wrinkle in the new emergency restrictions, however, which involves the two statutory sections (§§ 399-z and 399-pp) that are amended. Section 399-z defines "unsolicited telemarketing sales calls," as discussed above, and carves out calls made in response to a customer's express written or verbal request or under an established business relationship. Unlike Section 399-z, Section 399-pp does not define "unsolicited telemarketing sales calls."

Although it is reasonable under traditional methods of statutory interpretation to look for a term's use or meaning in other parts of the same or corresponding provisions, there is some ambiguity in the interplay between Sections 399-z and 399-pp. An aggressive reading of the restriction added to Section 399-pp would be that all telemarketing sales calls during the state of emergency are prohibited. A less extreme reading can be achieved by applying the definition of "unsolicited telemarketing sales calls" under Section 399-z to both sections. This exercise remains untested, and therefore presents some potential areas for exposure.

Impact: So long as New York is under a state of emergency, unsolicited telemarketing sales calls, whether manually or auto-dialed, may not be made unless the call recipient has provided consent or there is an established business relationship between the caller and call recipient, and consent has not been withdrawn. Once the state of emergency is lifted, New York's traditional telemarketing laws should apply, requiring consent (in the specific form provided under the statute) only for auto-dialed telemarketing sales calls. It is important to remember that additional opt-out requirements and restrictions on sharing of customer information have also recently been added to New York's telemarketing laws and apply regardless of any state of emergency.

To revoke or not revoke: Courts diverge as to whether consumers may revoke contractual consent to be called

Although consent to be called is generally revocable under the Telephone Consumer Protection Act (TCPA), two federal circuit courts of appeal have now held that a recipient of an autodialed phone call may *not* revoke consent where consent was included as a term in an underlying contract between the call recipient and the caller. Specifically, the Second Circuit, in *Reyes v. Lincoln Auto. Fin. Servs.*, 861 F.3d 51, 53 (2d Cir. 2017), followed more recently by the Eleventh Circuit, in *Medley v. Dish Network, LLC*, 958 F.3d 1063 (11th Cir. 2020), found that a consumer's consent to receive autodialed calls is irrevocable when given in connection with entering into a contract. These decisions are at odds with a 2013 decision from the Third Circuit in *Gager v. Dell Fin. Services, LLC*, 727 F.3d 265, 268 (3d Cir. 2013), as well as a number of district court decisions outside of the Second and Eleventh Circuits. Consumers' ability to revoke contractually provided consent thus remains an unsettled question, and largely dependent on jurisdiction.

Whether and in what form a consumer has given consent to be contacted via an automatic telephone dialing system (ATDS) may be a crucial aspect of determining liability under the TCPA. Consent may preclude certain TCPA claims since the TCPA prohibits certain types of calls, including those using an ATDS, to the extent that the caller does not have "the prior express consent of the called party." 47 U.S.C. § 227(b)(1)(A)-(B). Through the terms in some contracts, consumers explicitly consent to receive ATDS calls. The question of whether consumers can later change their minds and revoke that contractually agreed consent – thus subjecting the contractual counterparty to TCPA liability – is an issue that has wound its way to three U.S. Circuit Courts of Appeal.

In the 2013 Third Circuit decision in *Gager*, the court relied on common law principles to conclude that the TCPA affords a consumer the right to revoke prior express consent to be contacted on his cellular phone via an autodialing system, and the right to revoke consent may not be abridged by a contract. Significantly, the *Gager* court noted that, "[a]lthough … the level of contact that a debtor will consent to may be relevant to the negotiation of a line of credit, the ability to use an autodialing system to contact a debtor is plainly not an essential term to a credit agreement." 727 F.3d at 274.

Four years later, the Second Circuit took a different approach in *Reyes*. In that case, the court found that, as a matter of "black-letter" law, a party to a contract may not alter or revoke a term of a bilateral agreement. In the context of the TCPA, this led the court to conclude that a consumer cannot unilaterally revoke contracted-for consent to be called without the agreement of the other contracting (i.e., the calling) party.

Following *Reyes*, district courts outside of the Second and Third Circuits took divergent views on this issue. In one of those decisions, the Middle District of Florida agreed with *Reyes*, and dismissed a plaintiff's TCPA claim where the call recipient tried to revoke consent after providing it as a term of the contract. In that case, the plaintiff and DISH Network entered into a contract that allowed DISH to call the plaintiff using an ATDS. The Eleventh Circuit upheld summary judgment dismissal of the plaintiff's TCPA claim, joining *Reyes* in citing "black-letter" contract law prohibiting a party from unilaterally altering the terms of its contract. The *Medley* court noted that the plaintiff gave consent to be called as a "mutually-agreed-upon term in a contract," and nothing in the TCPA (or in the guidance issued by the Federal Communications Commission (FCC)) addressed, much less abrogated, that basic contractual principle. 958 F.3d at 1070. The court also distinguished the facts before it from a case where, for example, consent was

given as part of an application and not a signed contract and acknowledged that consent given gratuitously in an application may be revocable. *Id.*

Including consent provisions in consumer contracts may be a viable means of limiting exposure to the TCPA, but liability can be dependent on the jurisdiction in which the TCPA claim is litigated. Regardless, note that this issue is more relevant to non-marketing calls, such as collection calls, because many businesses include consent language in their standard form contracts. For marketing calls, however, the FCC rules preclude making consent a condition of purchase.

Federal TRACED Act and state laws aimed at combating robocalls

2019 saw an effort by both Congress and various state legislatures to reduce the volume of robocalling and "spoofed" calls. Robocalls are pre-recorded calls placed through automated dialing equipment while spoofed calls falsely appear to come from a particular area code or legitimate place of business to increase the recipient's chances of answering. Both have been the source of federal and state legislation in 2019 due to the surge of these practices throughout the country.

This alert provides a general overview of the federal Pallone-Thune Telephone Robocall Abuse Criminal Enforcement and Deterrence Act (TRACED Act) and also discusses several notable examples of state laws passed in 2019 aimed at reducing robocalling and spoofing.

The TRACED Act

The TRACED Act, signed into law by President Trump on December 30, 2019, provides additional consumer protections against robocalls. Notably, the TRACED Act allows for certain civil forfeiture penalties for Telephone Consumer Protection Act (TCPA) violations and up to $10,000 in additional penalties for intentional violations. The TRACED Act also provides the Federal Communications Commission (FCC) with additional time (from 2 years to 4 years) to bring actions for civil forfeiture penalties based on violations related to knowingly providing misleading or inaccurate caller ID information. Lastly, the TRACED Act requires the FCC to issue a number of reports, rules, and proceedings regarding a wide variety of issues affecting the telecommunications industry, such as spoofing and call authentication.

The TRACED Act, a bipartisan bill, first introduced in Congress in 2018, broadens FCC authority to levy TCPA civil penalties and extends the time period for the FCC to catch and take civil enforcement action against intentional violations. The new law will not put an immediate end to improper robocalling practices, which have been exacerbated in recent years due to the growing industry of "spoofing" technology, but will certainly cause individuals to think twice before engaging in illegal robocalling activity.

TRACED Act provisions include:

Civil forfeiture penalties: TCPA violations

- The TRACED Act adds two new subsections under the TCPA allowing for civil forfeiture penalties for violations of the TCPA's prohibitions against the use of automated telephone equipment under 47 U.S.C. § 227(b).
- Civil forfeiture penalties (under a 1-year statute of limitations) may be added on top of any other statutory penalty with an additional $10,000 in penalties (under a 4-year statute of limitations) for those who are determined by the FCC to have violated the TCPA *"with the intent to cause such violation."*
- Certain procedural protections are mandated, such as notice and an opportunity to be heard, before the FCC may impose these penalties, but other safeguards, such as the issuing of a citation prior to fining certain classes of alleged violators, are not required.

FCC reporting

Under the TRACED Act, the FCC is required to provide reports to Congress and/or the public on a myriad of telecommunications issues, such as:

- FCC enforcement efforts taken against robocalling, including the number of complaints received by the FCC, FCC-issued citations, amount of penalties and fines, and FCC proposals to reduce robocalling.

- Implementation efforts taken by voice service providers—which are required under the TRACED Act to enable the Secure Telephone Identity Revisited (STIR)/Secure (or Signature-based) Handling of Asserted Information Using ToKENs (SHAKEN) authentication technologies—aimed at blocking unauthenticated calls and cutting back on spoofed calls.
- The progress of setting up a reassigned number database, which the FCC must report on within 1 year of the TRACED Act's enactment.
- Efforts taken by voice service providers to determine the source of suspected robocalls as part of an annual robocall report by the FCC.
- Evidence of intentional robocall violations, which the FCC must report to the US Attorney General. The FCC must also provide the number and types of such violations via an annual, public summary.

FCC proceedings and working groups

The TRACED Act directs the FCC to initiate proceedings on specified topic areas as well as implement certain working groups to combat robocalling, including for example:

- Within 120 days of the TRACED Act's enactment, the FCC is required to initiate a proceeding regarding one-ring scams.
- The FCC is also required to initiate a proceeding regarding how it may reduce potential robocallers' ability to access phone numbers.
- As for working groups, the US Attorney General and Chairman of the FCC are instructed to form an interagency group to study TCPA prosecutions. The FCC must also create an advisory group specifically to address robocalling practices to hospitals

FCC rulemaking and regulations

Examples of additional FCC regulations required under the TRACED Act include:

- Rulemaking regarding spoofed calls from unauthenticated phone numbers.
- The addition of certain consumer protection requirements for specific categories of exemptions under the TCPA.
- Regulations to streamline private entities' abilities to provide information to the FCC regarding robocalls and spoofing violations.

2019 State Legislative Updates

At the state level, there were also a number of new legislative and regulatory initiatives focused on reducing the number of robocalls and spoofed calls.

A number of states—including Arkansas, California, New York, North Carolina, and Texas—pursued efforts to combat the use of misleading information provided to caller ID services in a concerted attempt to reduce spoofing.

A new law promulgated in Arkansas in April 2019, for example, designates spoofing as a felony and similarly increases criminal penalties in connection with robocalling to felonies. California has also sought to reduce robocalling and spoofing by mandating that telecommunications service providers have STIR/SHAKEN call authentication protocols or comparable technology put in place by January 1, 2021. And in New York, under its Nuisance Call Act signed into law in December 2019, telemarketers during live telemarketing sales calls are now required to offer consumers the choice to be added to the company's do-not-call list.

Conclusion

Like the TCPA, which is one of the most powerful consumer protection statutes of our era, these newly enacted laws are noteworthy examples of Congress and state legislatures providing greater protection to consumers against robocalling and spoofing.

The TRACED Act, a bipartisan bill, first introduced in Congress in 2018, broadens FCC authority to levy TCPA civil penalties and extends the time period for the FCC to catch and take civil enforcement action against intentional violations. The new law will not put an immediate end to improper robocalling practices, which have been exacerbated in recent years due to the growing industry of "spoofing" technology, but will certainly cause individuals to think twice before engaging in illegal robocalling activity.

Shaken and stirred—FCC adopts caller ID standards to combat illegal spoofing; definition of autodialer remains elusive

The FCC announced on March 31, 2020, new rules requiring implementation of caller ID authentication, known as STIR/SHAKEN.[1] The FCC is requiring voice service providers to implement caller ID authentication using the STIR/SHAKEN technical standards in the Internet Protocol (IP) portions of their networks by June 30, 2021 to protect consumers from "spoofing," a method used by scammers and some telemarketers to trick consumers into answering their phones. The long overdue and much needed definition of "autodialer" (also known as ATDS), however, remains elusive.

According to the FCC, STIR/SHAKEN enables phone companies to verify that the caller ID information that is transmitted with a call matches the caller's phone number. In the FCC's view, "[w]idespread deployment of STIR/SHAKEN will reduce the effectiveness of illegal spoofing, allow law enforcement to identify bad actors more easily, and help phone companies identify calls with illegally spoofed caller ID information before those calls reach their subscribers." According to FCC Chairman Ajit Pai, "spoofed" calls are among the hundreds of millions of daily unwanted calls that Americans receive. Chairman Pai explained that "[t]he caller spoofs or manipulates the caller ID information that appears on the recipient's phone to trick him into thinking that the call is from someone he knows or can trust."

Cast against the backdrop of the global coronavirus pandemic, Chairman Pai noted that spoofed calls prevent health care officials from making important phone calls, and in the past two weeks (since about mid-March), "utility companies from Maryland to California have warned about fraudsters spoofing their phone numbers and exploiting concerns about financial uncertainty during the pandemic, threatening to shut off service if customers don't pay up."

The June 2021 implementation deadline is consistent with the deadlines articulated in the recently enacted TRACED Act. The FCC also adopted a Further Notice of Proposed Rulemaking to accept public comments with respect to expanding the STIR/SHAKEN implementation mandate to apply to intermediate voice service providers; extending the implementation deadline by one year for small voice service providers; adopting requirements to promote caller ID authentication on voice networks that do not rely on IP technology; and further implementation of the TRACED Act.

Chairman Pai also scheduled a STIR/SHAKEN Robocall Summit for July 11 to examine the industry's progress toward meeting his deadline and to identify any challenges to the deployment of the STIR/SHAKEN framework and discuss how best to overcome them. In March 2020, the Commission adopted new rules requiring all originating and terminating voice service providers to implement caller ID authentication using STIR/SHAKEN technological standards in the Internet Protocol (IP) portions of their networks by June 30, 2021.

1 STIR/SHAKEN stands for Secure Telephone Identity Revisited (STIR)/Secure (or Signature-based) Handling of Asserted Information Using ToKENs (SHAKEN).

According to the FCC's news release on the rules:

> [T]he benefits of eliminating the wasted time and nuisance caused by illegal scam robocalls will exceed $3 billion annually, and STIR/SHAKEN is an important part of realizing those cost savings. Additionally, when paired with call analytics, STIR/SHAKEN will help protect American consumers from fraudulent robocall schemes that cost Americans approximately $10 billion annually. Improved caller ID authentication will also benefit public safety by reducing spoofed robocalls that disrupt healthcare and emergency communications systems.

The FCC further opined that implementation of STIR/SHAKEN "will restore consumer trust in caller ID information and encourage consumers to answer the phone, to the benefit of consumers, businesses, healthcare providers, and non-profit organizations."

In a separately issued statement, FCC Commissioner Michael O'Rielly expressed concern over the cost of implementing STIR/SHAKEN. He also addressed head-on the FCC's failure to-date to tackle one of the most vexing issues pending before the FCC, namely, the definition of "autodialer" under the TCPA, which continues to fuel large-dollar, bet-the-company TCPA class actions. Issuing a clarion call to his fellow FCC Commissioners, Commissioner O'Rielly stated:

> I hope we will finally have the will to respond to the D.C. Circuit's set-asides in *ACA International v. FCC* and clarify the TCPA's 'automatic telephone dialing system' provision. As long as the harmful and backwards *Marks v. Crunch San Diego* decision still stands, any efforts to enact blocking and labeling redress mechanisms for legitimate callers will be for naught if unscrupulous class action plaintiffs are able to flock to the 9th Circuit to serve legitimate businesses with abusive and frivolous TCPA lawsuits. Especially now that the 7th and 11th Circuits have explicitly rejected the approach in *Marks*, allowing the confusion and uncertainty to linger any longer is tremendously unfair to those legitimate companies trying to do the right thing. And, to the extent that the Commission isn't prepared to do this just yet, we must act on the over fifty petitions pending before the Commission for TCPA clarification and relief. Either way, the Commission must stop allowing legitimate callers to be unfairly punished by statutory misinterpretation and frivolous litigation.

Laudable as implementing STIR/SHAKEN is, Commissioner O'Rielly's comments hit the nail on the head and focus on the urgent and long overdue need for the FCC to issue guidance on the definition of autodialer and ATDS. Doing so will inform courts and guide the course of pending and future TCPA class actions, which have cost companies hundreds of millions of dollars.

Given the large number of TCPA class actions that continue to be filed, the FCC's ongoing delay in clarifying the TCPA autodialer rules has left the regulated community both shaken AND stirred.

Chairman Pai also scheduled a STIR/SHAKEN Robocall Summit for July 11 to examine the industry's progress toward meeting his deadline and to identify any challenges to the deployment of the STIR/SHAKEN framework and discuss how best to overcome them. In March 2020, the Commission adopted new rules requiring all originating and terminating voice service providers to implement caller ID authentication using STIR/SHAKEN technological standards in the Internet Protocol (IP) portions of their networks by June 30, 2021.

FCC adopts final rules implementing federal TRACED Act

The Federal Communications Commission (FCC) has set forth final rules pursuant to the federal Pallone-Thune Telephone Robocall Abuse Criminal Enforcement and Deterrence Act (TRACED Act), allowing for further civil forfeiture penalties for certain Telephone Consumer Protection Act (TCPA) violations. The FCC's rules were first adopted in an FCC order on May 1, 2020. The rules were published in the Federal Register on June 26, 2020, and become effective on July 27, 2020.

The TRACED Act became law on December 30, 2019, and provides consumer protections against robocalls, most notably through enhanced penalties and additional time for the FCC to bring certain enforcement actions. This alert serves as an update to our prior alert on the TRACED Act, which is available here.

The new rules amend the FCC's current rules on forfeiture proceedings to reflect the legislative changes that the TRACED Act made to the TCPA. The TRACED Act amended the TCPA in several respects, which the FCC has now adopted in its amended regulations (47 CFR § 1.80), such as:

- Removing the requirement that the FCC must first issue a citation to alleged violators of Section 227(b) of the TCPA who do not have an FCC-issued license, permit, certificate, or other authorization or who are not applicants for such authorization before the FCC can seek to impose a forfeiture penalty against such violators. Section 227(b) of the TCPA generally relates to the use of an automatic telephone dialing system or artificial or prerecorded voice.

The impact of the TRACED Act and the FCC's rules implementing its legislative changes, including how aggressively the FCC may pursue enforcement actions and penalties, largely remains to be seen, as the TRACED Act continues to add to the robust regulatory framework surrounding the TCPA.

- Adding civil forfeiture penalties with respect to *intentional* violations of Section 227(b) of the TCPA.[1] Per the TRACED Act and the FCC's new rules implementing the Act, those who the FCC finds to have violated Section 227(b) of the TCPA with intent may face a potential penalty up to $10,000 per intentional unlawful robocall. This is in addition to the existing penalties under the Communications Act (47 U.S.C. § 503(b)), which generally imposes liability for various activity, including certain willful or repeated violations with respect to holding an FCC license or other type of FCC-issued authorization as well as violations of telecommunications requirements, such as those involving broadcasting.[2]
- Increasing the statute of limitations for the FCC to bring an enforcement action for *intentional* violations of Section 227(b) of the TCPA from one year to four years.
- Increasing the statute of limitations for the FCC to bring an enforcement action relating to violations of Section 227(e) of the TCPA (Truth in Caller ID Act, relating to unlawful "spoofing" activity) from two years to four years.

The FCC considered its adoption of the new rules to be "largely ministerial" given that the FCC found its action to "simply effectuate[] regulations established by legislation and require[] no exercise of administration discretion." Therefore, the FCC adopted the rules without a notice and comment period, finding that the rules' adoption fell within the "good cause" exception to the Administrative Procedure Act.[3]

1 As a general matter, the TRACED Act allows for civil forfeiture penalties (under a 1-year statute of limitations) to be added on top of any other statutory penalty with an additional $10,000 in penalties (under a 4-year statute of limitations) for intentional violations.
2 *See* 47 U.S.C. § 503(b)(1).
3 May 1, 2020 FCC Order available here.

Conclusion

The impact of the TRACED Act and the FCC's rules implementing its legislative changes, including how aggressively the FCC may pursue enforcement actions and penalties, largely remains to be seen, as the TRACED Act continues to add to the robust regulatory framework surrounding the TCPA.

Permission required: FCC limits number of robocalls to residential phones without prior express consent

On December 30, 2020, the Federal Communications Commission (FCC) issued guidance in a Report and Order that limits the number of artificial or prerecorded voice calls that may be placed to residential phone lines absent the called party's prior express consent. Prior to the FCC's Report and Order, there was no limit on the number of such robocalls. The FCC's order does not affect the rules regarding calls to cell phones, which prohibit automated calls without the called party's prior express written consent. .

The FCC's Report and Order implements Section 8 of the Pallone-Thune Telephone Robocall Abuse Criminal Enforcement and Deterrence (TRACED) Act, which was signed into law in 2019. The TRACED Act amended provisions of the Telephone Consumer Protection Act (TCPA) and required the FCC to issue further guidance as to the specifics of the Act.

Under the FCC's newly announced rules:

- Callers may place a maximum of three calls to residential lines within a consecutive 30-day period for non-commercial purposes using an artificial or prerecorded voice. The same limit applies to calls made for non-telemarketing commercial purposes.
- Callers from tax-exempt nonprofit organizations may place up to three calls using an artificial or prerecorded voice within a consecutive 30-day period.
- HIPAA-related calls are limited to one artificial or prerecorded voice call per day, but no more than three calls per week.

In addition, call recipients retain the right under the TCPA to opt out of calls covered under the TRACED Act. Callers must also provide either a callback number for customers to opt out or provide an automated interactive voice or keypad opt-out process. Unlike calls to cell phones where the caller must obtain some form of consent before placing the call (and the required form of consent varies depending on whether the call is for marketing or non-marketing purposes), callers to residential lines may request consumer consent during an approved call. With consent, the presumptive limit on the number of calls does not apply.

Companies that communicate with their customers or prospective customers through multiple channels should pay particular attention to the new rules. The limitation on calls applies specifically to calls made by or on behalf of an entity. Inadvertence and inattention could trigger liability under the TCPA.

The FCC's rule becomes effective six months from the date of publication of the Office of Management and Budget's approval of the rules in the Federal Register.

FCC releases new guidance on autodialers, leaves key questions unanswered

Although the hunt for a workable definition of autodialer (automatic telephone dialing system, or ATDS) continues, a calling platform must be "capable of originating a call or sending a text" without human intervention in order to qualify as an autodialer under the Telephone Consumer Protection Act (TCPA), according to a June 25, 2020 declaratory ruling from the Federal Communications Commission (FCC).[1] In issuing its ruling, the FCC conspicuously avoided addressing other key autodialer issues under the TCPA, leaving litigants to continue to grapple with a growing split among federal courts across the country. What constitutes an autodialer—and therefore what types of telecommunications devices may be subject to the TCPA—has been at the heart of *thousands* of lawsuits filed over the past few years. Over the past year, multiple federal circuit courts have issued diverging opinions with the Second and Ninth Circuits aligning to define autodialer broadly, and the Third, Seventh, and Eleventh Circuits taking a narrower, more business friendly, view. Meanwhile, the FCC comment period aimed at developing new rules closed more than a year-and-a-half ago, and the FCC's June 2020 ruling leaves the final chapter – and the elusive definition of autodialer – still unwritten.

The key question underlying the dispute over the definition of autodialer is whether the TCPA applies to a dialing system that can call from a stored list of numbers, or whether the TCPA's autodialing restrictions are instead limited to systems that have the capacity for random or sequential number generation, as the plain language of the statue indicates. Numerous federal appellate courts have considered the issue, and the split in the law is deepening. In light of the TCPA's statutory damages provision that allows for $500 per violation (and treble damages for reckless or intentional violations), plus attorneys' fees with no cap on damages, this lack of clarity is particularly concerning in the context of potential class action liability.

The FCC confirms that a manual dialing platform is not an autodialer

The FCC's June 2020 declaratory ruling states that manual dialing is not autodialing—a proposition that should be obvious by common sense, but which has been muddied by the general uncertainty surrounding the autodialer definition. In response to a petition filed by a coalition of peer-to-peer text messaging services (P2P), the FCC ruled that a calling system is not an autodialer if it is "not capable of originating a call or sending a text without a person actively and affirmatively manually dialing each [call or text]" A manual dialing system per this order will "require a person to manually send each text message [or call] one at a time."

The June 2020 ruling is helpful in providing guidance on a range of manual dialing platforms, particularly those that improve the efficiency of manual calling, such as one-touch calls or individual text messages using templates. The FCC reiterated that the autodialer restrictions do not apply to functions such as "speed dialing," where the caller places the call without dialing all of the digits, because this type of system requires human intervention. Likewise, the FCC rejected arguments that a system's ability to make a large volume of calls is a factor in identifying an autodialer. This was a point

1 FCC Declaratory Ruling, In the Matter of Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991, P2P Alliance Petition for Clarification, CG Docket No. 02-278 (June 25, 2020).

made in opposition to the petition by several commentators, who argued that peer-to-peer text platforms are used to send "massive numbers of texts in tiny periods of time" and that "the individual involvement in sending these messages is so vanishingly small as to be meaningless." But the FCC found that the volume of calls or texts is not dispositive, provided that the system requires the calls or texts to be placed manually, one at a time. Stated differently, a system is not an autodialer if it "lacks the capacity to transmit more than one message without a human manually dialing each recipient's number."

Federal circuit courts are split on the autodialer standard

Meanwhile, the FCC's ruling on manual dialing conspicuously avoided wading into the larger and more significant dispute over systems that can dial from lists of stored numbers, and whether such calls are prohibited by the TCPA without prior express consent. Federal appellate courts across the country have taken up this question, reaching divergent answers, and the US Supreme Court may be poised to take up the issue.

The TCPA defines the term an autodialer as "equipment which has the capacity—(A) to store or produce telephone numbers to be called, using a random or sequential number generator; and (B) to dial such numbers."[2] Although this statutory definition may seem clear enough, the TCPA was passed nearly thirty years ago and, unsurprisingly, does not adequately address contemporary issues presented by current and emerging telecommunications technology. This has led to a long history of twists and turns in the interpretation of the definition. Regulators, courts and business have continued to struggle with the foundational TCPA question of what constitutes an "automatic telephone dialing system" under the statute.

In a 2015 order, the FCC expanded the definition of an ATDS to encompass any equipment that has the capacity or potential capacity to dial numbers without human intervention, even if the caller does not use the device in that capacity or the device requires an upgrade to have those features. In early 2018, however, the FCC's definition was struck down by the D.C. Circuit Court of Appeals as arbitrary and capricious, and the FCC solicited comments so it could develop a new rule. More than a year-and-a-half has now passed without FCC action, and while the FCC remains silent, federal courts have filled the breach.

The key issue involves the application of the TCPA to systems that dial from lists of stored numbers, specifically, whether the TCPA applies to systems that can "store numbers to be called" from a list, or whether the restrictions apply only to systems that "use a random or sequential number generator" when storing or producing numbers. In 2018, the Ninth Circuit Court of Appeals articulated a broad standard, holding that an ATDS is a device with the capacity "to store numbers to be called" and to dial such numbers automatically after the system is initiated by a person.[3] More recently, the Second Circuit expressly adopted the Ninth Circuit's approach, holding that a system is an autodialer if it places calls from stored lists.[4]

Other appellate courts, however, have adopted a narrower definition of autodialer and have held that an ATDS must have the capacity to use a random or sequential number generator, as required by the plain language of the statute. The Eleventh Circuit Court of Appeals came down strongly in favor of this narrow standard, holding that an ATDS must: (1) use a random or sequential number generator either to store or produce telephone numbers; and (2) dial the numbers.[5] The Third Circuit, and most recently the Seventh Circuit, have also adopted this narrow interpretation. As the Seventh Circuit stated, to be an autodialer "a device must be capable of performing at least one of those functions [storing or producing numbers] using a random or sequential number generator."[6]

Given the stark split among the circuit courts of appeal, the United States Supreme Court may be the final arbiter of the issue, and particularly if the FCC fails to issue new rules or guidance. Pending before the Supreme Court is a petition for writ of certiorari in *Facebook, Inc. v. Noah Duguid*, Case No. 19-511, a highly watched case from the Ninth Circuit that presents the Court with the opportunity to address the autodialer issue. One of the specific questions on appeal is whether the definition of an ATDS encompasses any device that can "store" and "automatically dial" telephone numbers, even if the device does not use a random or sequential number generator, the issue that defines the split among the circuits. With the Supreme Court's recent decision upholding the constitutionality of the TCPA, in *Barr v. American Association of Political Consultants*, No. 19-631 (July 6, 2020), the *Facebook* case could continue the trend of the Court taking at least one TCPA case per term. If the Supreme Court grants certiorari, we anticipate the Court will address this long-unresolved question that goes to the heart of the TCPA.

2 47 U.S.C. § 227(a)(1).
3 *Marks v. Crunch San Diego, LLC*, 904 F.3d 1041, 1053 (9th Cir. 2018).
4 *Duran v. La Boom Disco, Inc.*, 955 F.3d 279, 283 (2d Cir. 2020).
5 *Glasser v. Hilton Grand Vacations Co., LLC*, 948 F.3d 1301 (11th Cir. 2020).
6 *Gadelhak v. AT&T Servs., Inc.*, 950 F.3d 458, 468-69 (7th Cir. 2020) (finding device did not constitute ATDS where it did not have "capacity to generate random or sequential numbers"); *Dominguez v. Yahoo, Inc.*, 894 F.3d 116, 121 (3d Cir. 2018).

Conclusion

Eversheds Sutherland Observation: The search for a clear definition of an ATDS under the TCPA continues, and the answer remains elusive. The FCC's June 2020 ruling is a helpful step forward in further confirming that manual dialing is not autodialing, but key questions remain. The business community remains hopeful that the FCC or the courts, including the United States Supreme Court, will finally provide a long-awaited clarity in 2020 that businesses can rely on to understand what constitutes an autodialer and under what circumstances the TCPA will and will not apply.

Eversheds Sutherland Observation: The search for a clear definition of an ATDS under the TCPA continues, and the answer remains elusive. The FCC's June 2020 ruling is a helpful step forward in further confirming that manual dialing is not autodialing, but key questions remain. The business community remains hopeful that the FCC or the courts, including the United States Supreme Court, will finally provide a long-awaited clarity in 2020 that businesses can rely on to understand what constitutes an autodialer and under what circumstances the TCPA will and will not apply.

FCC releases new guidance on liability for fax senders: You are (sometimes) your brother's keeper

On September 21, 2020, the Federal Communications Commission (FCC) issued a declaratory ruling[1] clarifying the liability of "senders" of faxes under the Telephone Consumer Protection Act of 1991 (TCPA).[2] The ruling makes clear that a fax broadcaster is solely liable for TCPA violations arising from faxing on behalf of an advertiser if the broadcaster engages in fraudulent or deceptive conduct, including breaching a contract to fax on behalf of an advertiser.[3] Although this finding narrows the potential liability for advertisers who engage third-party broadcasters to transmit faxes, the FCC was clear that advertisers will still remain liable for TCPA fax violations in many circumstances. Although limited in scope, the FCC's ruling is important for companies that engage third-party fax broadcasters to transmit fax advertisements on their behalf, and a positive development for advertisers (and broadcasters) that operate in good faith and in compliance with the TCPA.

Background

The TCPA prohibits the use of "any telephone facsimile machine, computer or other device to send, to a telephone facsimile machine, an unsolicited advertisement," with certain limited exceptions, such as where the party sending the fax has a prior relationship with the recipient or the recipient has expressly granted permission to receive the fax.[4] The fax sender is generally defined as "the person or entity on whose behalf a facsimile unsolicited advertisement is sent or whose goods or services are advertised or promoted in the unsolicited advertisement."[5] The fax broadcaster is defined as "a person or entity that transmits messages to telephone facsimile machines on behalf of another person or entity for a fee."[6]

In its declaratory ruling issued in September 2020, the FCC provided further clarification on the liability standards for fax senders. The ruling is a long-awaited response to the law firm Akin Gump Strauss Hauser & Feld LLP's 2019 petition seeking guidance on the definition of sender, and elaborates on a portion of the FCC's 2006 Junk Fax Order. The 2006 Order states that "[i]n most instances" the sender will be "the entity whose products or service is advertised or promoted" by the fax.[7] Akin Gump sought clarification as to whether an advertiser that is "stripped of [its] ability to control the fax campaign or ensure compliance with the TCPA" because of a fax broadcaster's "deception, fraud, blatant contract violations and misrepresentations," is still liable or, rather, whether because of the fax broadcaster's actions the advertiser is no longer considered the "sender" of the fax and, therefore, only the fax broadcaster is liable under the TCPA.

1 *In the Matter of Akin Gump Strauss Hauer & Feld LLP Petition for Expedited Clarification or Declaratory Ruling Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991 Junk Fax Prevention Act 2005*, 2020 WL 5747205 (Sept. 21, 2020) [hereinafter, "Ruling"].
2 Telephone Consumer Protection Act of 1991, Pub. L. No. 102-243, 105 Stat. 2394, § 2(9) (1991), codified at 47 U.S.C. § 227(b)(1)(C)
3 Ruling at *1
4 47 U.S.C. § 227(b)(1)(c)
5 47 CFR § 64.1200(f)(10)
6 47 C.F.R. § 64.1200(f)(6)
7 *Junk Fax Prevention Act of 2005*, CG Docket Nos. 02-278 and 05-338, Report and Order and Third Order on Reconsideration, 21 FCC Rcd 3787, 3808 (2006) [hereinafter, "2006 Junk Fax Order").

FCC Offers Guidance on "Senders" under the TCPA

The FCC's ruling finds that a fax broadcaster may be exclusively liable for sending a fax under certain circumstances. Specifically, a broadcaster may be "solely liable for TCPA violations when it engages in deception or fraud against the advertiser"[8] where the advertiser is "unaware of and unable to prevent unlawful faxes."[9] The ruling provides an example from one of the FCC's prior orders in which a fax broadcaster wins business from an advertiser by falsely claiming to have consent from prospective fax recipients. Under such circumstances, the FCC has held that the advertiser has been deceived by the broadcaster, and therefore only the fax broadcaster would be liable for any TCPA violation.

In the ruling, the FCC gives two other relevant and real-life instances, both from cases in the US Court of Appeals for the Seventh Circuit. In *Bridgeview Health Care Center v. Clark*, 816 F.3d 935 (7th Cir. 2016), an advertiser provided approval for a fax broadcaster to send faxes to 100 businesses within 20 miles of the advertiser's location. However, the fax broadcaster sent faxes to 5,000 telephone numbers in three states. The Seventh Circuit concluded that under the circumstances the broadcaster did not send the faxes "on behalf of" the advertiser, and therefore, the advertiser was not liable under the TCPA. Similarly, in *Paldo Sign & Display Co. v. Wagener Equities, Inc.*, 825 F.3d 793 (7th Cir. 2016), the Seventh Circuit similarly found that where a fax broadcaster had contracted with a commercial real estate company, promising to gain consent before faxing any advertisements, and the broadcaster failed to do so, the advertiser could not be held liable under the TCPA.

8 Ruling at *1
9 Ruling at *3

While the ruling is a positive development for businesses that advertise through faxing, the FCC emphasized that the ruling should not be interpreted as a loophole for advertisers to dodge liability simply by outsourcing its fax advertising. Indeed, the FCC held that an advertiser will still face liability under the TCPA if it directs unauthorized conduct or is aware of ongoing unlawful conduct by the fax broadcaster. Further, if the advertiser consents to the conduct or fails to take action to prevent further known misconduct by the broadcaster, the advertiser may also be found liable. In other words, companies that contract with fax broadcasters cannot take a 'hear no evil, see no evil' approach to suspected TCPA violations by third-party broadcasters without potentially running afoul of the TCPA.

Conclusion

The September 21 ruling provides clarification for third-party liability in the context of faxing, and may also signal a renewed effort by the FCC to further clarify the bounds of the TCPA.

Dialing In: TCPA Top 5 Issues for 2021

Will anything stop the continuing barrage of class action lawsuits under the Telephone Consumer Protection Act (TCPA)? In 2020, TCPA lawsuits remained one of the most commonly-filed type of class action in federal courts across the country, and all signs indicate that the trend will continue in the year ahead. Yet potential changes loom on the horizon. The United States Supreme Court is poised to issue a decision that could dramatically impact hundreds of pending cases involving alleged autodialers and alter the TCPA landscape for good. New leadership at the Federal Communications Commission (FCC) could revise or clarify TCPA rules, and courts across the country continue to grapple with various issues regarding the scope and potency of the statute. Here, we discuss the TCPA Top 5 issues for 2021

1. The Supreme Court might (finally) tell us what an autodialer is.

Courts and businesses alike continue to struggle with the foundational TCPA question of what constitutes an automatic telephone dialing system (ATDS or autodialer). The question has finally reached the U.S. Supreme Court, in *Facebook, Inc. v. Noah Duguid*, and the Court is expected to issue its opinion in the coming months.

The history of the autodialer issue goes back decades to the 1991 enactment of the TCPA, but the significance of the question has come into sharp focus over the past five years. In a 2015 Order, the FCC expanded the definition of ATDS to encompass any equipment that has the capacity or potential capacity to dial numbers randomly or sequentially, even if the company does not use the device in that capacity or the device requires an upgrade to have those features. In early 2018, however, the FCC's definition was struck down by the U.S. Court of Appeals for the D.C. Circuit. The FCC subsequently solicited comments from the public in order to develop a new rule, but the FCC has held off on setting a new standard despite the importance of the issue to hundreds if not thousands of pending matters in courts across the country.

Since the D.C. Circuit's decision in 2018, some courts have moved partly back toward the FCC's 2015 definition in finding that an ATDS can be a device that automatically dials numbers from a list, even if a random or sequential number generator is not used.[1] Other courts, however, have held that an ATDS must have the capacity to *generate* numbers, which is a narrower interpretation seemingly more faithful to the plain language of the statute.[2] These courts have held that to be an ATDS, the calling system must: (1) use a random or sequential number generator either to store or produce telephone numbers; and (2) dial the numbers.[3]

Is a device that simply stores and dials telephone numbers an ATDS, or must the device also use a random or sequential number generator? That is the question the Supreme Court stands to answer in 2021 with a decision in the *Facebook* case. The fate of hundreds of pending class actions hangs in the balance, as plaintiffs could face a much higher – in some cases, insurmountable – hurdle in prosecuting their claims.

1 *Marks v. Crunch San Diego, LLC*, 904 F.3d 1041, 1053 (9th Cir. 2018).
2 *See* e.g., *DeCapua v. Metro. Prop. & Cas. Ins. Co.*, No. 18-00590-WES, 2019 WL 4757995, at *3 (D. R.I. Sept. 30, 2019); *Denova v. Ocwen Loan Servicing*, No. 8:17-cv-2204-T-23AAS, 2019 WL 4635552, at *4 (M.D. Fla. Sept. 24, 2019); *Reed v. Quicken Loans, Inc.*, No. 3:18-cv-3377-K, 2019 WL 4545010, at *2 (N.D. Tex. Sept. 3, 2019); *Adams v. Safe Home Sec. Inc.*, No. 3:18-cv-03098-M, 2019 WL 3428776, at *4 (N.D. Tex. July 30, 2019).;
3 *E.g., Glasser v. Hilton Grand Vacations Co.*, LLC, 948 F.3d 1301 (11th Cir. 2020).

2. Impact of a new administration and a reconstituted FCC

The change of presidential administrations in January 2021 will result in an immediate change at the FCC. Chairman Ajit Pai, who has served as chair for four years, has announced that he will leave the FCC in January. With Pai's departure, the FCC would be left with four members—two Democrats and two Republicans—until the Senate confirms a new member nominated by the incoming Biden administration. Even before a new commissioner is installed, however, the Biden administration can designate one of the sitting Democrats as the new chair, so that control of the FCC's agenda will shift parties.

For the TCPA, the policy implications of the shift are as yet uncertain. Companies impacted by TCPA litigation risk had hoped that Republican control over the past four years would have resulted in more business-friendly rules—at a minimum to provide more clarity on permitted calling practices, if not also to get some relief from class action exposure based on technical violations. Those hopes mostly did not come to pass, and key issues remain unresolved (*e.g.*, the FCC never issued new rules clarifying the definition of autodialer) and the wave of class actions has continued largely unabated.

It is unlikely that a reconstituted FCC would be in favor of loosening TCPA rules. Nonetheless, any additional guidance that clarifies gray areas would be helpful for businesses seeking to comply with the TCPA.

3. When does a plaintiff have standing to file a TCPA claim?

Does receipt of a single call or text constitute an "injury" sufficient for a plaintiff to file a TCPA lawsuit in federal court? What about two calls or texts? Is a momentary annoyance really enough injury to open the doors to a federal courthouse?

Federal appellate courts are reaching differing conclusions on standing, setting this up as a key issue to watch in 2021. Some courts have held that the receipt of one or two unsolicited calls or texts is a sufficient injury in facts to confer standing.[4] But other courts are questioning whether such a minimal event really constitutes an "injury." In 2019, a panel of the Eleventh Circuit held that the receipt of a single unsolicited text message did not amount to an "injury in fact" sufficient to establish Article III standing to bring a TCPA lawsuit.[5] The court found that the plaintiff's allegations, reflecting nothing more than a momentary annoyance, did not generate the harm necessary to support a claim in federal court. In a subsequent case, however, a different panel of the Eleventh Circuit opined that receiving "more than one unwanted telephone call" could be an injury in fact, and that the named plaintiff, who had asked not to be called, had alleged an injury traceable to the defendant's alleged failure to maintain an internal do-not-call list.[6] In a 2020 decision, a third panel in the same Circuit noted that "the point is close" as to whether even receipt of two calls is sufficient for standing.[7]

These cases touch on an area in TCPA law that warrants further clarification by the courts in 2021, specifically, delineating the types of harm and the degree of harm required to establish standing to bring a TCPA claim. Courts are scrutinizing whether cases alleging a small number of texts or calls are subject to dismissal for lack of standing. The injury question is also potentially significant at the class certification stage if the alleged class contains individuals who may lack standing.

4. Who's calling? Standards for third-party liability under the TCPA

Companies that market products through third-party agents or distributors face a particular risk under the TCPA when their agents call, text, or fax consumers without obtaining the necessary consent. TCPA cases often implicate issues of vicarious liability when a third party initiated the communications on behalf of another party. Courts generally apply traditional agency principles in cases involving telephone calls and text messages. The TCPA makes it unlawful "to initiate" certain telephone calls and text messages, and both the FCC and courts have agreed that traditional agency principles govern the application of third-party or vicarious liability. The 2013 FCC declaratory ruling, *In re Dish Network*, 28 FCC Rcd. 6574 (2013), has been interpreted to establish that a person who does not physically initiate a telephone call, but rather relies on a third party to do so, may be held liable under the TCPA under the common law of agency, based on actual approval, apparent authority and ratification. Subsequent cases have applied the vicarious liability standard articulated in *In re Dish Network* to assess third-party liability under the TCPA.

4 *Van Patten v. Vertical Fitness Group, LLC*, 847 F.3d 1037, 1043 (9th Cir. 2017) (receipt of two allegedly unsolicited text messages constituted an injury in fact).
5 *Salcedo v. Hanna*, 936 F.3d 1162 (11th Cir. 2019).
6 *Cordoba v. DIRECTV, LLC*, 942 F.3d 1259 (11th Cir. 2019).
7 *Glasser v. Hilton Grand Vacations Co.*, 948 F.3d 1301, 1306 (11th Cir. 2020).

With the proliferation of online lead generators and multi-channel marketing, class actions involving multiple parties are more and more common in the TCPA space. Some complaints allege vicarious liability based on the actions of third parties that may be far removed from the acts of one or more of the other defendants, who may have had no involvement in the allegedly unlawful telemarking. District courts are scrutinizing these allegations at the motion to dismiss stage, particularly where a plaintiff is not able to draw a clear connection between the various parties.[8] In other cases, the relationships between the parties may raise multiple questions of fact. We expect courts will continue to evaluate the bounds of third-party TCPA liability in multiple new cases over the next year.

5. Was the TCPA unconstitutional before 2020?

A small number of recent lower court decisions have called into question whether the autodialer prohibitions of the TCPA were unconstitutional—and therefore unenforceable—between 2015 and 2020. If this position gains traction in the courts, it could wipe away hundreds of pending TCPA lawsuits across the country that allege autodialing violations.

The theory for unconstitutionality is based on the U.S. Supreme Court's 2020 decision in *Barr v. AAPC*,[9] which struck down a robocalling exception for government debt-collection calls that had been enacted by Congress in 2015. In *AAPC*, the Court held that the government debt-collection exception was an unconstitutional content-based restriction under the First Amendment. The Court declined to strike down the TCPA's robocalling restrictions in their entirety—as the petitioners were requesting—and instead applied severability principles to invalidate only the debt-collection exception while leaving the remainder of the statute intact. The result was that the bulk of the TCPA's autodialing provisions are enforceable after the Supreme Court's ruling in July 2020.

In a series of recent cases, however, defendants have argued that the existence of the unconstitutional provision with the robocalling portion of the statute rendered the entire robocalling section unconstitutional until the constitutionality of the statute was restored by the Supreme Court in July 2020. The first federal district courts to consider the issue agreed with the defendant and dismissed complaints that alleged robocalling violations that occurred before 2020.[10] More recently, several district courts have gone the other way,[11] with more courts set to consider the issue in 2021, including possible appeals of these early decisions. This is a key issue to watch that could have an enormous impact on litigation over pre-2020 calls and texts.

Conclusion

TCPA cases remained one of the most common types of class action in 2020, and that trend is expected to continue as 2021 gets underway. Plaintiffs' lawyers will continue to target many different industries, and a strong TCPA compliance program is essential to help businesses of all kinds avoid TCPA lawsuits and potential exposure.

8 *E.g.*, *Bilek v. Fed. Ins. Co.*, No. 19 C 8389, 2020 WL 3960445, at *6 (N.D. Ill. July 13, 2020) ("[Plaintiff] does not allege that [defendant] had control over the quality, timing, and volume of calls, as well as the geographic location of customers to be targeted."), *appeal docketed*, No. 20-2504 (7th Cir. Aug. 12, 2020); *Rogers v. Postmates Inc.*, No. 19-CV-05619-TSH, 2020 WL1032153, at *4 (N.D. Cal. Mar. 3, 2020) ("[E]ven if the sender was authorized to market on [defendant's] behalf, there are no factual allegations suggesting that [defendant] knew or reasonably should have known that the sender of the text or any of its agents or sub-agents were violating the TCPA on its behalf.").
9 *Barr v. Am. Ass'n of Political Consultants, Inc*, 140 S. Ct. 2335 (July 6, 2020).
10 *Creasy v. Charter Commc'ns, Inc.*, No. CV 20-1199, 2020 WL 5761117 (E.D. La. Sept. 28, 2020).
11 *Shen v. Tricolor California Auto Grp., LLC*, No. CV 20-7419 PA (AGRX), 2020 WL 7705888, at *4 (C.D. Cal. Dec. 17, 2020).

For further information

If you would like to learn more about Eversheds Sutherland's TCPA compliance and litigation team, contact us.

Lewis Wiener
Chair, Partner
Washington DC
T: +1 202 383 0140
lewiswiener@eversheds-sutherland.com

Wilson Barmeyer
Partner
Washington DC
T: +1 202 383 0824
wilsonbarmeyer@eversheds-sutherland.com

Frank Nolan
Partner
New York
T: +1 212 389 5083
franknolan@eversheds-sutherland.com

Alexander Fuchs
Counsel
New York
T: +1 212 389 5082
alexfuchs@eversheds-sutherland.com

Valerie Strong Sanders
Counsel
Atlanta
T: +1 404 853 8168
valeriesanders@eversheds-sutherland.com

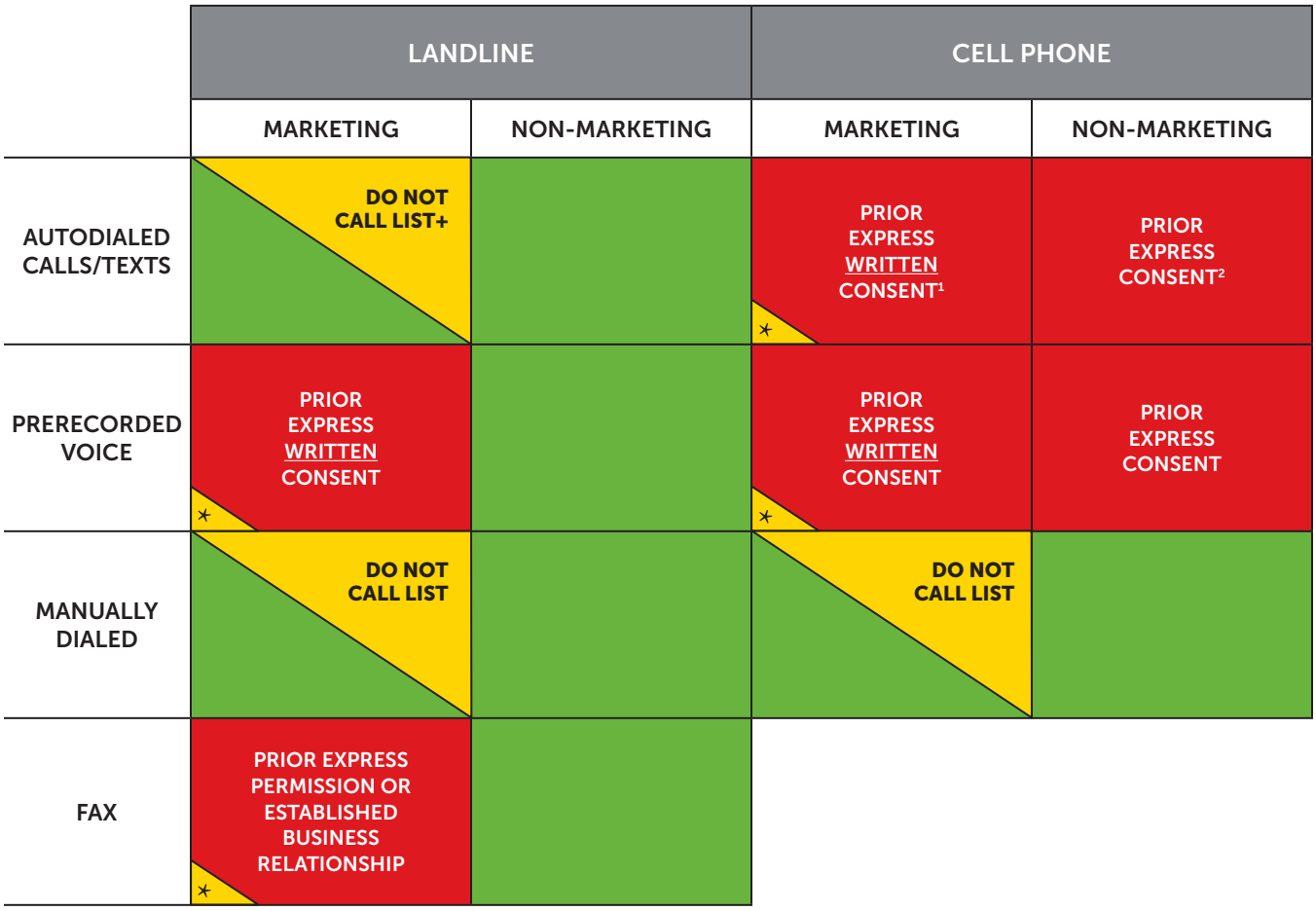
Samir Aguirre
Associate
Washington DC
T: +1 202 383 0974
samiraguirre@eversheds-sutherland.com

Emily Bork
Associate
Washington DC
T: +1 202 383 0870
emilybork@eversheds-sutherland.com

Melissa Fox
Associate
Atlanta
T: +1 404 853 8109
melissafox@eversheds-sutherland.com

Jessica Rodgers
Associate
Washington DC
T: +1 202 383 0152
jessicarodgers@eversheds-sutherland.com

The TCPA traffic light



[1] "Prior express written consent" requires a written agreement, signed by the consumer, that includes, among other things, the telephone number that specifically authorizes telemarketing by automatic dialing/texting or prerecorded voice, and that is not required as a condition of purchase. 47 C.F.R. § 64.1200(f)(8).

[2] For non-marketing purposes, providing a cell number in connection with a transaction generally constitutes prior express consent to be contacted at that number with information related to the transaction. 7 F.C.C.R. 8752 ¶ 31 (1992).

+ Do Not Call List restrictions apply broadly to telemarketing to both cell phones and landlines, but can be overridden by written consent from the consumer.

* Opt-out notice and mechanism must be provided. Specific requirements vary.

This chart does not constitute legal advice. ***This chart provides only a general overview of TCPA rules and does not reflect all details needed for compliance.***

eversheds-sutherland.com

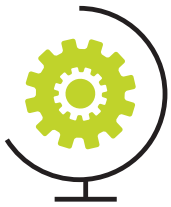
Why work with us?

As a purpose-led organization, we are proud of our culture and the values that guide our behavior.

Our purpose:

Helping our clients, our people and our communities to thrive.

Our values:



Collaborative

We leverage our collective talents for the benefit of our clients and each other and we prize teamwork and relationships.

Creative

We are innovative and creative problem-solvers, providing an enhanced client and employee experience by not being bound by custom or convention.

Professional

We deliver quality and excellence and act with the utmost integrity at all times.

Inclusive

We foster a diverse and inclusive culture that places respect and support for everyone at its core and empowers all our people to fulfill their potential.

Open

We are approachable and nurture a culture of transparency and openness.