FINTECH MEETS THE TELEPHONE CONSUMER PROTECTION ACT

David Goodfriend* and David Nayer*

Cite as: 1 GEO. L. TECH. REV. 446 (2017)

https://perma.cc/9B3U-89BN

INTRODUCTION

It could happen any time—at work, at home, or on vacation. You receive a text message and glance at your smartphone. Your bank-issued credit card provider just sent you a message asking if you recognize a recent transaction. "Did you authorize a purchase of $5,000 for Super Bowl tickets? Text 1 for YES, 2 for NO." You remember using your card to purchase tickets to an NBA playoff game but not to the Super Bowl. You reply, 2, and your credit card provider suspends the transaction. This text message may have saved you a significant amount of money and alerted you to possible identity theft. However, your card provider may have exposed itself to financial liability—not for the security breach, but for the unsolicited text message.

Fraud alerts from financial institutions are a classic application of "fintech," the increasingly prevalent application of modern technology to enhance financial services.[1] Many fintech uses, including the above example, implicate the Telephone Consumer Protection Act (TCPA), a law passed in 1991 intended to prevent potentially unwanted, automated marketing calls.

---

* J.D., *cum laude*, Georgetown ('97); Adjunct Professor, Georgetown University Law Center; President, Goodfriend Government Affairs.

* Georgetown University Law Center class of 2017; B.A., History & Political Science, University of Michigan 2014.

[1] *See FinTech*, FINTECH WEEKLY, https://fintechweekly.com/fintech-definition (last visited Mar. 30, 2017) [https://perma.cc/JP5Y-NTYX].

While some of these communications, like the example above, may benefit the consumer, many are a source of frustration. Nearly 100,000 complaints of violations of the Do-Not-Call list were filed at the FCC in 2014, and amounting to forty percent of FCC consumer complaints.[2] A fraud alert from a bank-issued credit card delivered via an automated outbound text message to a customer generally falls within the scope of what TCPA regulates but, as discussed below, the definitions of key terms in the TCPA have not always kept up with technology.

Recent action by the Federal Communications Commission ("FCC") in establishing requirements for the behavior of financial institutions in circumstances like the fraud alert illustrates how telecommunications laws and policies have been slow to keep up with fintech developments. The story of fintech regulations shows how the advocacy of industry groups and consumer representatives can lead to compromises that seem to miss the mark. Current policy outcomes can be explained by regulators balancing opposing political perspectives instead of looking at the actual use of the technologies in question. This should come as no surprise to veterans of the administrative advocacy process, but the implications may be very real for fintech providers and consumers.

A BRIEF INTRODUCTION TO THE TCPA

The TCPA, as amended, and including its implemented FCC regulations, provides consumers with numerous protections from potentially unwanted telemarketing and automated calls.[3]

Consent—and the requirement to seek it—is the lynchpin of TCPA liability. For all covered communications, the caller must receive prior express consent from the recipient to avoid liability.[4] Covered communications include telemarketing or advertising messages,[5] but communications under emergency circumstances are exempt.[6] Text messages are treated as calls in

[2] *See* DISSENTING STATEMENT OF COMMISSIONER AJIT PAI (June 18, 2015), https://apps.fcc.gov/edocs_public/attachmatch/FCC-15-72A5.pdf [https://perma.cc/LF6H-XTW9].
[3] *See* 47 U.S.C. § 227; *see also* 47 § C.F.R. § 64.1200.
[4] *See* 47 U.S.C. § 227(b)(1)–(2); *see also* 47 C.F.R. § 64.1200 (a)(1)–(3).
[5] *See* 47 C.F.R. § 64.1200(a)(2).
[6] *See* 47 U.S.C. § 227(b)(1)(A); *see also* 47 C.F.R. § 64.1200(a)(1).

the TCPA.[7] Consent requirements also vary depending on the recipient, with wireless numbers generally subject to more protection from covered communications than residential landlines.[8] The statute prohibits covered communications made with an artificial or pre-recorded voice (popularly known as robocalls)[9] to both wireless and residential wireline numbers.[10] Covered communications to wireless numbers made using an autodialer, equipment that can produce and call numbers using a number generator, are prohibited without prior express consent.[11] For those calls that are permitted, the TCPA lays out further restrictions to minimize their invasiveness.[12]

The FCC may exempt from consent requirements certain wireless calls not charged to the wireless customer and with such conditions as may be necessary to protect the customer's privacy.[13] This includes ensuring that text messages do not count against plan minutes or text message limits.[14]

---

[7] *See* In the Matter of Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991, CG Docket No. 02-278, *Declaratory Ruling and Order*, 18 FCC Rcd. 14014, ¶ 165 (2003).

[8] *See* In the Matter of Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991, CG Docket No. 02-278, *Declaratory Ruling and Order*, 30 FCC Rcd. 7961, ¶ (2015) [hereinafter *Omnibus Order*].

[9] "Robocall" is used casually throughout the Omnibus Order, and is applied synonymously with calls that "require consumer consent" under the TCPA. *See Omnibus Order* at ¶ 1 & n.1.

[10] *See* 47 U.S.C. § 227(b)(1)(A)(iii) and (b)(1)(B). Many Americans will note the prevalence of these artificial calls in the run-up to an election. By rule, robocalls to a residential line do not require consent if they are made on behalf of a tax-exempt organization, or if they do not constitute advertising or telemarketing. 47 C.F.R. § 64.1200(a)(3). However, artificial calls are also subject to further restriction; they must state the name of the calling entity at the beginning of the message. During the message, the call must state a telephone number. Solicitations must, within two seconds of stating the number, provide an automated, voice or key-activated opt-out system. 47 C.F.R. § 64.1200(b).

[11] 47 U.S.C. § 227(b)(1)(A)(iii). The statute also prohibits autodialers from targeting emergency services and hospital guest rooms, which may better illustrate the overall purpose of the restrictions. 47 U.S.C. § 227(b)(1)(A). As with robocalls, the consent requirement for autodialed calls is lifted if the message does not include advertising or telemarketing, or is made with the prior express written consent of the called party or the prior express consent of the called party when the call is made by or on behalf of a tax-exempt organization. 47 C.F.R. § 64.1200(a)(2).

[12] Further restrictions include compliance with the National Do-Not-Call Registry (notably maintained by the Federal Trade Commission, not the FCC), maintenance of an internal do-not-call list and acceptance of call recipients' desire not to be called again, and a prohibition on solicitations made outside the hours of 8 a.m.–9 p.m. in the recipient's time zone. 47 C.F.R. § 64.1200(b), (c).

[13] 47 U.S.C. § 227(b)(2)(C).

[14] *See Omnibus Order* at ¶ 127 (citing *Cargo Airline Order*, 29 FCC Rcd 3432 at *3, ¶ 12).

The FCC enforces the TCPA and has promulgated regulations implementing the above protections. In addition to these agency remedies, the TCPA also creates a private right of action, so individuals may enjoin or recover actual monetary damages (with a minimum of $500 per violation) from TCPA violators, "if otherwise permitted by the laws or rules of court of a State."[15] Most enforcement actions are brought in federal court and the damages can be enormous. Courts tend to apply FCC interpretations of the TCPA in determining the meaning of the statute.[16]

EVOLUTION OF THE TCPA – 2015 OMNIBUS DECLARATORY RULING

Likely resulting from plaintiffs invoking judicial jurisdiction, stakeholders have come to the FCC seeking backward-looking declaratory rulings, rather than forward-looking, prophylactic rulemakings. In comparison to the rulemaking process, these declaratory rulings are disruptive, giving them unusually powerful implications across multiple industries, including financial services.

The latest example of this backward-looking approach is the FCC's latest major interpretations of the TCPA, the 2015 TCPA Omnibus Declaratory Ruling and Order, combining twenty-one requests for clarification of various TCPA rules.[17] This ruling is currently being challenged in the D.C. Circuit by a group of nine plaintiffs.[18] While there are many issues raised and addressed in this Declaratory Ruling, three particularly interest financial services providers—the definition of autodialer, the expansion of the consent requirement, and the creation of a safe harbor for certain types of messages from financial institutions.[19]

---

[15] 47 U.S.C. § 227(b)(3).

[16] *See* Brief for Respondents at 39-40, ACA Int'l, et al., v. Fed. Commc'n Comm'n (D.C. Cir. Jan. 15, 2016) (No. 15-1211) (citing Nat'l Cable & Telecomm. Ass'n v. Brand X, 545 U.S. 967, 980 (2005) and Chevron U.S.A., Inc. v. Natural Resources Defense Council, 467 U.S. 837 (1984)). *See also* 28 U.S.C. § 2342(1). Because all appeals from final orders of the FCC must be heard in an appellate court, potential liabilities are higher for TCPA stakeholders.

[17] *See Omnibus Order* at ¶ 2.

[18] Brief for Respondents at § i, ACA Int'l, et al., v. Fed. Commc'n Comm'n¸ (D.C. Cir. 2016) (No. 15-1211).

[19] *See Omnibus Order* at ¶ 2.

Predictive Autodialers

The Omnibus ruling attempted to clarify the definition of autodialing technology, which, as discussed above, is prohibited from calling emergency services and wireless numbers absent sufficient consent. Petitioners sought clarification as to whether "equipment used to make a call is an autodialer subject to the TCPA only if it is *capable* of storing or generating sequential or randomized numbers *at the time of the call*,"[20] (emphasis added).

The FCC stood by its functionality-based interpretation of the TCPA's autodialer definition, affirming that "dialing equipment generally has the capacity to store or produce, and dial random or sequential numbers (and thus meets the TCPA's definition of 'autodialer') even if it is not presently used for that purpose, including when the caller is calling a set list of consumers."[21] Commenters (now Petitioners-appellants) contested the Commission's statutory interpretation and argued that the definition of "capacity" was overbroad and limitless, and it could even extend to smartphones that store numbers in a directory and can make a pre-programmed, outbound call.[22] The FCC disagreed, reasoning that the record included no evidence of individual customers being sued under the TCPA for use of a smartphone, the scenario raised by petitioners.[23]

In the opening example of the automated fraud alert text message, the sender of the text message generally uses predictive algorithms to identify transactions outside of a consumer's normal behavior and automated equipment to send an outbound text message to the consumer. Although the FCC has concluded that the use of such techniques generally meets the FCC's definition of "autodialer," plaintiffs challenging the FCC's interpretation argue that the definition is too vague as to future applications of the rule, rendering the Order both unconstitutional for its vagueness,[24] and impractical for compliance purposes. Defenders of the FCC decision argue that the FCC upholds Congress' stated intent in passing the TCPA as demonstrated by Congressional validation of the broad regulatory approach[25] made to best

[20] *See Omnibus Order* at ¶ 11.
[21] *Id*. at ¶¶ 11-12.
[22] *Id*. at ¶¶ 20-21.
[23] *Id*. at ¶ 21.
[24] *See* Brief for Respondents at 69, ACA Int'l v. Fed. Commc'n Comm'n (D.C. Cir. Feb. 24, 2016) No. 15-1211.
[25] *See id*. at 66.

capture as many intended technologies as possible.[26] Thus, while sending a fraud alert via text message arguably could violate the TCPA's consent requirements, it is difficult if not impossible to predict how future technological message-sending technologies might or might not trigger TCPA requirements.

Changes to the Consent Requirement

The FCC's Omnibus Order also tackled questions related to the establishment, revocation, and transferability of consent.[27] When a customer transfers her preferred method of communication with a company to a wireless device, the prior express consent remains intact despite the transfer to a new device.[28] By contrast, if a wireless number is reassigned to a new subscriber, the original consumer's consent does not transfer and callers may be liable, but for a one-call window intended to allow callers that do not have actual knowledge of the reassignment to seek necessary consent.[29] The FCC also noted that because the TCPA is silent on the revocability of consent, the FCC interprets this absence in a light most favorable to consumers—consumers may unconditionally revoke their consent at any time.[30] The Omnibus Order also ruled that simply having a contact in a phone's address book alone does not grant prior express consent to receive messages from the contact under the TCPA.[31]

These alterations to the consent regime also have been challenged by appellants as a violation of the Administrative Procedures Act and an impractical solution.[32] Appellants argue that complying with the requirement to allow consumers to revoke consent by any reasonable method is unworkable, and therefore the regulation is arbitrary and capricious.[33] Allowing customers to revoke consent in any way that a court later determines is reasonable arguably places an impractical burden of individualization and prevents callers from adopting a uniform cancellation policy.

---

[26] *See Omnibus Order* at ¶ 16 (citing 1992 TCPA Order, 7 FCC Rcd at ¶ 6).
[27] *See id.* at ¶ 47.
[28] *See Omnibus Order* at ¶ 54.
[29] *See id*. at ¶¶ 75-90.
[30] *See id*. at ¶ 56.
[31] *See id*. at ¶ 52.
[32] *See* Brief for Petitioners at 53-56, *Fed. Commc'n Comm'n* , No. 15-1211 (D.C. Cir. Jan. 15, 2016).
[33] *See id*. at 74.

Financial Institutions' Safe Harbor

In a decision directed expressly at the financial services industry, the FCC's Omnibus Order established a free-to-end-user safe harbor for financial institutions' use of text messages and voice calls to consumers for non-telemarketing, non-advertising messages. Responding to a petition by the American Bankers Association ("ABA"), the FCC exempted from the prior express consent requirement, within limited conditions, certain messages about time-sensitive financial issues.[34]

The Order specified that financial institutions[35] need not obtain prior consent to robocall or text message the customer if such calls or texts:

1. Are free to the user; meaning the call or text does not count against any wireless plan limits, such as minutes or text caps;[36]
2. Are limited to content concerning (a) alerts about fraud or identity theft; (b) alerts of possible security breaches of a customer's personal information; (c) messages about steps customers can take to prevent or remedy harm caused by a data security breach; and (d) actions needed to arrange for receipt of pending money transfers;[37]
3. Are sent only to the wireless number provided by the customer of the financial institution;
4. State the name and contact information of the financial institution;
5. Do not include any telemarketing, cross-marketing, solicitation, debt collection, or advertising content;
6. Are limited to one minute or less for voice, 160 characters or less for text messages;
7. Number no more than three messages over a three-day period per event;
8. Offer recipients an easy "opt out" option to avoid such communications in the future, which in the case of text messages must be the ability to respond "STOP;" and

[34] *See Omnibus Order* at ¶¶ 128-39.
[35] *Omnibus Order* at ¶ 127 n.424. For purposes of the safe harbor, "financial institution" means any institution in the business of providing financial services "as described in section 4(k) of the Bank Holding Company Act of 1956."
[36] *See id*. at ¶ 139.
[37] *See id*. at ¶¶ 128-33.

9. In the event a consumer opts out, the financial institution honors that request immediately.[38]

The FCC justified this safe harbor on the time sensitivity of the use cases in question and the speed at which consumers tend to open text messages.[39] Citing record evidence, the FCC noted that "seconds count" in situations where fraud may be occurring,[40] and that similar time sensitivity exists where data security breaches or identity theft may have occurred.[41] It noted the "urgency" of the situation, the "unpredictable timing" of the problem, and the "financial repercussions" at stake.[42] Similarly, with respect to money transfers, senders and recipients may not have engaged in such transfers in the past and verification in real time is necessary, an "exigency" the FCC found to be time-sensitive.[43]

The FCC relied on evidence submitted by the ABA that 98% of text messages are opened within three minutes of receipt, justifying text messaging as the ideal communications platform for financial institutions' time-sensitive communications.[44]

In the case of the Super Bowl ticket purchase fraud alert discussed above, if a customer receives an alert of possible fraud from a financial institution, such messages would have to conform with the FCC's TCPA consent exemptions (unless the institution had already received prior consent). The message must be: free to the customer, with zero impact on her phone bill; within one of the Order's four content categories discussed in the second item above, in this case a fraud alert; sent to the wireless number provided by the customer; sent with the name and contact information of the financial institution; within prescribed length and frequency limits; free of any telemarketing, cross-marketing, solicitation, debt collection, or advertising; and sent with the "STOP" opt-out.

---

[38] *See id*. at ¶ 138.
[39] *Omnibus Order* at ¶ 128. Although not discussed in this article, the safe harbor exception also applies to certain healthcare-related messages for similar reasons.
[40] *Omnibus Order* at ¶ 129.
[41] *See id*. at ¶ 129.
[42] *See id*. at ¶ 130.
[43] *See id.*
[44] *See id*. at ¶ 128 (citing ABA Petition at 5).

ADVOCACY BEHIND THE FINANCIAL INSTITUTIONS SAFE HARBOR

The safe harbor exemption for certain exigent financial-services messages potentially saves financial institutions from massive liabilities, presumably improving the service that they provide to their customers, but the exemption is subject to some seemingly random conditions, such as the three-calls-over-three-days limit. The administrative process and advocacy through which the safe harbor arose explain some of these peculiarities and illustrate how public policy often results in compromise between adversarial parties, to the complete satisfaction of none.

The ABA's initial request for a declaratory ruling set out the four situations under which it sought an exemption from prior notice requirements and offered limitations on the use of such communications.[45] The FCC quoted directly from the ABA's petition,[46] and adopted many of its recommendations nearly verbatim.[47]

However, the ABA was not acting in a vacuum. The National Consumer Law Center, a non-profit consumer advocacy organization specializing in TCPA and financial services issues, opposed the ABA petition, arguing that if the text messages concerned real emergencies, then such messages would fall within the well-established emergency exemption for prior consent and would not require any further safe harbor.[48] It also argued that financial institutions could secure prior consent to make calls or send texts in certain circumstances, rendering a safe harbor unnecessary.[49] In the event that the FCC adopted the ABA's proposed safe harbor, however, NCLC argued for stricter limitations than those proffered by ABA, such as a limit on the number of communications and an easy opt-out option.[50]

The FCC seems to have struck a compromise. It adopted the ABA's requested safe harbor but tempered it with the NCLC-recommended easy opt-out and cap on the number of calls or messages (i.e., no more than three calls

---

[45] *See* Petition for Exemption of the American Bankers Association at 3, (Oct. 14, 2014) (No. 02-278), https://www.fcc.gov/ecfs/filing/60000972167 [https://perma.cc/HBF3-RHDG].
[46] *See Omnibus Order* at ¶ 127 (quoting ABA Petition at 3).
[47] *See Omnibus Order*, *supra* note 26 at 29.
[48] *See* Letter from Margot Saunders, Counsel, Nat'l Consumer Law Ctr., to Marlene Dortch, Sec'y, FCC (Dec. 19, 2014), https://www.nclc.org/images/pdf/energy_utility_telecom/telecommunications/comments-aba-petition-2014.pdf [https://perma.cc/MN9A-WL8W].
[49] *See id*. at 5.
[50] *See id*.

or messages over a three-day period for any given event).[51] The ABA originally had argued against any cap on calls or text messages, such as that established in a prior declaratory ruling, pointing to the importance of reaching the customer in exigent circumstances and noting that institutions had no incentive to send repeated messages other than to alert a customer to protect his or her assets.[52]

According to individuals involved in the deliberations, FCC staff sought NCLC's agreement to a certain number of calls or texts within a given time frame, to which NCLC ultimately acquiesced, despite having originally argued against any safe harbor. This is consistent with a statement made by the ABA in one of its final ex parte filings, in which it stated that an agreement had been reached with consumer advocates.[53] Although the ABA originally argued that there should be no limit on the number of contacts to ensure that consumers were reached, ultimately the FCC imposed the cap of three messages over a three-day period.[54]

The cap on calls or texts, while adapted from earlier precedent, appears to be a middle ground position unrelated to the on-the-ground facts and is disfavored by the affected parties—the banks, which do not want a cap,[55] and the consumer advocates, which did not support the safe harbor device in the first place.[56] Moreover, to ensure that text messages are "free" to the recipient, the consumer's wireless provider—not the financial institution instigating the message—ultimately has discretion. A financial institution must have an agreement in place with every wireless provider to ensure that safe-harbor communications are free to all recipients. A failure by the wireless carrier to comply places the financial institution outside of the safe harbor and thus subject to liability. This is a tenuous chain of responsibility for a financial institution seeking the benefit of the safe harbor.

NCLC's argument that emergency communications already are exempt from the prior notice requirement begs the question, why not simply deem the four situations to be emergencies outside the scope of the prior-consent requirement? This would have afforded the financial institutions

---

[51] *See Omnibus Order* at ¶ 135.
[52] *See Omnibus Order* at ¶ 134 (citing *Cargo Airline Order*, 29 FCC Rcd 3432 at 5, ¶ 18).
[53] *See generally* Letter from Charles H. Kennedy, Counsel, Am. Bankers Ass'n, to Marlene H. Dortch, Sec'y, FCC (May 22, 2015), https://ecfsapi.fcc.gov/file/60001048638.pdf [https://perma.cc/3BFV-Z9QN].
[54] *See Omnibus Order* at ¶ 135.
[55] *See* Petition for Exemption, *supra* note 45, at 18.
[56] *See* Letter from Margot Saunders, *supra* note 48 at 4-5.

sufficient clarity, if that is what they sought, without the detailed restrictions imposed in the ruling. Consumer advocates logically could wonder, given this easier option, whether motives in addition to liability protection might have animated the ABA proposal.

THE FUTURE OF THE TCPA

The future of these and associated rules *writ large* is uncertain. The D.C. Circuit is reviewing aspects of the 2015 ruling and could remand all or parts of the order back to the FCC for reevaluation. Then-FCC Commissioner, now Chairman Ajit Pai issued an exhaustive dissent alongside the Omnibus Order, which many of the appellants cited in their brief and echo in theory.[57]

Under the new leadership of Chairman Pai, the FCC could take a less restrictive view of the consent requirement, easing the regulatory burden on financial institutions to spend resources achieving that consent. On the other hand, the safe harbor could remain unchanged. Even on remand from the D.C. Circuit, Chairman Pai—a former Senate staff member and student of politics—could decide that there are too many political risks to reversing entirely what could be characterized as "anti-robocall" rules. Chairman Pai even acknowledged in his dissent that "fraudulent telemarketing" is a problem, one that he has experienced personally.[58] In his first speech after being named Chairman, Pai restated his feelings on telemarketing and suggested that the FCC should make it easier for consumers to report robocalls and for the FCC to take action.[59] Ahead of his March 23, 2017 FCC Open Meeting, Chairman Pai previewed an agenda item aimed at reducing unwanted robocalls.[60] He called upon the FCC to take further action to prevent these calls. The proposed rules empower the private sector, giving carriers tools to block calls that come from unassigned numbers. Regardless of how the TCPA may be altered by judicial or administrative decisions,

---

[57] *See* DISSENTING STATEMENT OF COMMISSIONER AJIT PAI, *supra* note 2.
[58] *Id*. at 1.
[59] *See* Adam Bender, *Pai Wants 'Aggressive Action' Against Robocallers, He Tells CAC; NAB Talks Up ATSC 3.0,* COMM. DAILY (Jan. 30, 2017), http://www.communicationsdaily.com/article/view?s=136854&id=513936 [https://perma.cc/99PL-8356].
[60] *See* Ajit Pai, *Springing Forward in the Public Interest: The FCC's March Agenda*, MEDIUM (Mar. 2, 2017), https://medium.com/@AjitPaiFCC/springing-forward-for-the-public-interest-the-fccs-march-agenda-337b8ef582bc#.6tbgj6a2n [https://perma.cc/W7V8-T4NT].

however, the statute and fintech surely will continue to intersect, especially as technological innovations in financial transactions proliferate.