Debevoise & Plimpton

Debevoise In Depth

OCC Issues Revised TCPA Examination Procedures: What Bank Compliance Personnel Should Know

November 15, 2023

On November 1, 2023, the Office of the Comptroller of the Currency (the "OCC") issued Bulletin 2023-35 (the "OCC Bulletin"), which contains revised interagency examination procedures (the "Procedures") for the Telephone Consumer Protection Act (the "TCPA"). The revisions, which were made by the OCC, Federal Deposit Insurance Corporation ("FDIC"), and the National Credit Union Administration ("NCUA"), reflect amendments to the TCPA that became effective on October 25, 2021. The OCC applies the Procedures to national banks, federal savings associations, covered savings associations, and federal branches and agencies of foreign banking organizations. With the publication of the Procedures, the OCC also rescinded the "Telephone Consumer Protection Act and Junk Fax Protection Act" section of the "Other Consumer Protection Laws and Regulations" booklet of the Comptroller's Handbook.

The TCPA regulates calls and text messages placed using certain types of automated dialers and artificial or prerecorded messages (among other things). The Procedures provide a useful update to the OCC's framework for ensuring that banks engaged in practices subject to the TCPA have the appropriate personnel, policies, and procedures in place to ensure any automated communications are carried out in a compliant manner, and that any potential gaps are remediated in a timely fashion. In particular, the OCC Bulletin highlights three aspects of the Procedures: (i) revocation of consent; (ii) a limited special exemption for banks disseminating fraud alerts; and (iii) a safe harbor related to use of a reassigned number database maintained by the Federal Communications Commission. We will discuss these issues below.[1]

---

[1] This update provides an overview of key TCPA obligations solely for informational purposes; an entity which engages in automated communications should consider having its practices reviewed by counsel periodically to ensure ongoing compliance with all applicable federal and state regulations. We do not discuss calls to residential telephone lines and communications via fax, both of which are addressed in the Procedures. We should also note that there may be circumstances where an entity deviates from the best practices described here, but nonetheless has viable defenses to TCPA claims, including in an enforcement context.

Takeaways for Banks

As banking organizations consider revisions to their policies in light of the Procedures, they should also consider conducting a full review of their TCPA compliance practices, potentially guided by experienced counsel with a sophisticated understanding of both TCPA compliance and the banking industry. Developing a robust TCPA compliance program is critical for two reasons: it mitigates the risk of (i) costly TCPA class action litigation and (ii) enforcement by the OCC, FDIC, NCUA, and Federal Communications Commission ("FCC"). Issuance of the Procedures suggests that bank examiners are likely to focus more on banks' TCPA compliance practices. Banks that are found to have significant deficiencies in TCPA controls may be subject to informal or formal enforcement actions, potentially even in the absence of customer complaints or litigation.

Calls and Text Messages to Cellular Telephones

The TCPA prohibits placing calls or text messages to a cellular telephone using either (i) a device that qualifies as an automatic telephone dialing system ("ATDS"), or (ii) an artificial or prerecorded voice, unless the calling party obtains prior express consent—which must be in writing if the call is placed in connection with telemarketing activities (among other things). If an entity retains a vendor to place calls or text messages on its behalf, that entity may be held liable for TCPA violations committed by the vendor. The TCPA provides for statutory penalties of $500 per unlawful call or text, with treble damages for willful violations.

Due to large statutory penalties, TCPA litigation typically presents significant financial risk. There is a cottage industry of law firms that specialize in filing putative TCPA class action lawsuits alleging that defendants placed large numbers of calls subject to the TCPA without prior express consent. These lawsuits frequently target entities engaged in telemarketing or debt collecting. Such lawsuits typically seek costly settlements from defendants which can range, in some cases, from millions to tens of millions of dollars. If an institution can demonstrate that it has a strong TCPA compliance program, that pivotal fact can be incorporated into an effective litigation strategy that may result in a TCPA claim being defeated outright or resolved on favorable terms.

What Types of Calls and Text Messages to Cellular Telephones Are Subject to the TCPA?

ATDS

The types of devices that fall within the definition of ATDS have been hotly debated. As described here, as a result of a 2021 Supreme Court opinion, the definition of an ATDS should include only dialers that were commonly in use at the time of the TCPA's enactment in 1991 that randomly or sequentially generated telephone numbers and then called those numbers. Automated dialers that place calls or text messages to lists of phone numbers of specific customers should not fall within the definition of an ATDS. Nonetheless, prudence dictates obtaining the requisite consent before placing any type of automated call or text message, including that: (i) some courts have accepted creative, albeit erroneous, attempts by plaintiffs to stretch the definition of what counts as an ATDS—particularly at early stages of litigation; (ii) certain state "mini-TCPA" laws encompass all types of automated dialing; and (iii) as discussed below, placing a call or text message without consent to someone on the national "Do Not Call" list may violate the TCPA.

Artificial or Prerecorded Voice

Calls involving a recorded voice message—including calls placed via an automated dialer that leaves voicemail messages—are potentially subject to the TCPA (depending on the circumstances).

How Does a Bank Obtain Consent for Telemarking Purposes?

A bank that places calls or texts using an ATDS, or calls using a prerecorded voice message, in connection with telemarketing activities must first obtain prior express written consent from each recipient of such calls or texts. The Procedures emphasize that a written agreement must contain a "clear and conspicuous disclosure," clearly stating that (i) by entering into the agreement, the counterparty is agreeing to receive telemarketing calls via ATDS or prerecorded voice, and (ii) entering into the agreement is not a condition for purchasing goods or services. Written consent can be obtained via an electronic signature, to the extent that this form of signature is recognized as valid under the applicable federal or state law. Banks should have detailed procedures to ensure that written consent is obtained where necessary and that proof of each such consent is memorialized and readily accessible in the event of litigation or an examination by the OCC. Banks who obtain consent via websites may wish to consider using third-party vendors who have specialized software that memorializes consent.[2]

---

[2] If calls are made for debt collection purposes, the calling party need obtain only prior express consent; such consent need not be written. Depending on the circumstances, the provision of a cellular telephone number to a creditor operates as consent for the creditor (or a vendor acting on its behalf) to place calls for debt collection purposes. Nonetheless, it is prudent to obtain written consent for risk mitigation purposes.

Banks should also have protocols in place to enable customers to revoke consent. The Procedures highlight that it will be examining such protocols. For compliance purposes, banks should assume that consent can be revoked through any reasonable means. This includes written and oral revocation. Banks should consider developing processes to facilitate and track customers' revocation of consent—and should not create any impediments to revoking consent. Note also that, in certain circumstances, customers must be given the opportunity to opt out of receiving such calls or text messages at the time that the telemarketing message itself is delivered. Once a customer revokes consent, all automated communications to that party should generally cease.

What Is the FCC's Safe Harbor for Avoiding TCPA Violations and When Is It Applicable?

One of the challenges presented by the TCPA is that it is a strict liability statute, meaning that a calling party can be liable if it places a call or text subject to the TCPA which reaches a non-consenting party for any reason—including reasons that are completely out of the calling party's control. TCPA lawsuits are frequently predicated on the allegation that a defendant has a practice of calling "wrong numbers" or other types of non-consenting customers. Although there are no sure-fire solutions to this problem, banks should consider incorporating risk mitigation strategies into a TCPA compliance program, including the following:

- The Procedures discuss a limited TCPA safe harbor for reassigned numbers. There is no TCPA liability if a calling party can demonstrate that: (i) it originally obtained the requisite prior express consent from the user of a particular telephone number; (ii) before making the call, it queried the Reassigned Numbers Database and received a report that the number had not been permanently disconnected subsequent to prior express consent having been obtained; yet (iii) the report was in error and the telephone number had in fact been reassigned.

- There is no safe harbor for calls placed to wrong numbers due to other types of errors, including clerical data entry errors. Banks may wish to consider using third-party vendors who conduct name / number matches and flag likely mismatches between the consenting customer and the telephone number at issue. Out of an abundance of caution, when there is a question regarding whether a consenting customer actually uses the telephone number associated with his or her record, the bank may wish to consider placing the call via a live agent who manually dials the telephone number.

Under What Circumstances May Banks Place Informational Calls or Texts to Their Customers with Fraud Alerts?

Banks are allowed to place calls or text messages using an ATDS or prerecorded voice to customers—even if they have not provided the requisite prior express consent—provided that a series of criteria have been satisfied in their entirety, including the following:

- The call or text message is not charged to the called person or counted against the called person's limits on calls or text messages.
- The bank places the call or delivers the message because: (i) a transaction and risk circumstances suggest a possibility of fraud or identity theft; (ii) there is a possible breach of a customer's personal information; (iii) the bank wishes to communicate the steps that can be taken to prevent or mitigate harm arising from data security breached; or (iv) certain actions are needed to facilitate pending money transfers. The messages may not include any telemarketing, solicitation, advertisement, or debt collection content.
- The bank may only send the message or make the call to the telephone number provided by the customer to the institution.
- The disclosure must state the name and contact information of the financial institution.
- The message must be concise.
- The bank may not initiate more than three messages per event per account over a three-day time period.
- The bank must give each customer an easy way to opt out of future messages and honor all opt-out requests immediately.

Do Not Call Regulations

Banks should also ensure compliance with the regulations governing "Do Not Call" ("DNC") lists.

- **Nationwide DNC List**. A bank should not deliver any telephone solicitation or telemarketing call or text to anyone who places themselves on the nationwide DNC list. A bank, however, will not violate the TCPA by placing such a call or text if it is

placed with the requisite consent. Additionally, in certain circumstances, a party may place a call or text message not subject to the TCPA (i.e., one placed by a live agent) to a customer on the nationwide DNC list who meets the definition of an "existing business relationship," provided that the customer has not made a DNC request to the calling party.

- **Internal DNC List**: Each bank should maintain its own internal DNC list, which memorializes the name and number of each customer who requests not to receive telemarking calls. The bank should have appropriate policies and procedures to ensure that DNC requests are memorialized and honored for at least five years.

The OCC's Expectations for Banks Engaging in Telemarketing

The Procedures instruct the OCC's examiners to assess the quality of a bank's TCPA compliance program through the following steps (among others):

- Assessing the strength of internal TCPA controls and procedures through the review of organizational charts; process flowcharts; policies and procedures for detecting potential violations and monitoring third-party vendors; disclosures and notices; and databases that track consent and opt-outs;
- Analyzing the adequacy of the institution's TCPA training procedures;
- Reviewing the adequacy of the institution's TCPA auditing and monitoring procedures, including management's responses to any identified gaps; and
- Conducting transaction-level testing—including a review of call logs, call scripts, and call recordings to assess the institution's TCPA compliance.

* * *

Please do not hesitate to contact us with any questions.

Helen V. Cantwell
Partner, New York
+1 212 909 6312
hcantwell@debevoise.com

Courtney M. Dankworth
Partner, New York
+1 212 909 6758
cmdankworth@debevoise.com

Maura Kathleen Monaghan
Partner, New York
+1 212 909 7459
mkmonaghan@debevoise.com

Caroline N, Swett
Partner, New York
+1 212 909 6432
cnswett@debevoise.com

Jacob W. Stahl
Counsel, New York
+1 212 909 6874
jwstahl@debevoise.com

Emma Macfarlane
Associate, New York
+1 212 909 7409
ekmacfarlane@debevoise.com