LEECHTISHMAN
LEECH TISHMAN FUSCALDO & LAMPL

Opportunistic TCPA Claims Call for Careful Examination, Vigorous Defense

By: Michael H. Sampson, Esq. and James K. Paulick, Esq.

Despite the U.S. Supreme Court's favorable ruling in *Facebook, Inc. v. Duguid*, 141 S Ct. 1163 (2021), cases alleging that businesses violated the federal Telephone Consumer Protection Act ("TCPA") and/or similar state statutes by making unauthorized telephone calls and/or sending unsolicited text messages continue to be filed. Often brought by opportunistic plaintiffs, these cases call for a careful examination and a vigorous defense.

No business should just accept the allegations made in a TCPA case (or, for that matter, in any action) at face value. Instead, if sued for allegedly violating the TCPA and/or a comparable state statute(s), a business should consider promptly taking the following "top ten" steps:

1

The business should engage experienced defense counsel – familiar with the law and the relevant technology – who can assist with the investigation and the defense of the lawsuit. Investigations generally should be conducted under the auspices of counsel to hopefully shield the work product from discovery. The business and/or its counsel may also decide to retain an expert(s) to assist with a forensic investigation.

2

Taking into consideration the specific facts alleged, the business and its counsel should carefully review the TCPA and any applicable state statute(s) to ensure they have a full understanding of all potentially relevant statutory prohibitions, defenses, and definitions.

3

If and as necessary, the business should determine whether it (or any vendor it engaged) actually used an "automatic telephone dialing system" ("ATDS") – as that term is used in the statute(s) and interpreted in Facebook – to make calls or to send text messages. Plaintiffs often just assume the business used an ATDS; in contrast, the business should determine whether an ATDS was in fact used. A technical understanding of the relevant system(s) will be important.

4

The business also should confirm that it (or a third-party acting on its behalf) in fact did make a call(s) or send a text message(s) to the plaintiff. The business should not just rely on the plaintiff's representations to that effect or assume that the plaintiff's counsel conducted a thorough investigation prior to a complaint being filed. At the same time, the business should determine whether it has any evidence that the plaintiff "opted in" to receiving such calls and/or such messages. Unfortunately, too often a plaintiff "forgets," or fails to disclose, that he or she in fact consented to receiving calls or text messages.

For assistance with the Telephone Consumer Protection Act or related litigation, please contact Michael H. Sampson or James K. Paulick.

Mike is a Litigation Partner with Leech Tishman and leads the Insurance Coverage Group, and is a member of the Data Privacy & Cybersecurity Group. He can be reached at msampson@leechtishman.com or 412.261.1600.

James is a Litigation Counsel with Leech Tishman and Leader of the Data Privacy & Cybersecurity Group, and is a member Emerging Cyber Technologies Industry Group. He can be reached at jpaulick@leechtishman.com or 424.738.4400.

LEECHTISHMAN
LEECH TISHMAN FUSCALDO & LAMPL

5

In consultation with counsel, the business should issue a "document hold," preserving relevant records (including, but not limited to, electronic records).

6

The business should ascertain whether it had any prior, or has any ongoing, business relationship with the plaintiff, and when, if it can be determined, that relationship began and/or ended. For example, the business should determine whether the plaintiff ever made any purchase(s) from the business. If so, the business also should identity and collect any records it has with respect to that relationship and any commercial interactions with the plaintiff. It should do a "deep dive;" for example, the business may need to determine whether someone else at the plaintiff's address (for example, a spouse) made a purchase(s) and/or authorized the calls or the messages.

7

If and as relevant, the business also should determine whether it has any records showing that the plaintiff actually ever "opted out" from receiving such calls or text messages, or any records of any communications at all with the plaintiff. Again, a business should not just take the plaintiff's word for it. This examination may require follow-up with any vendors the business used to place calls or send messages.

8

The business should review its commercial contracts to determine, among other considerations, whether a third-party vendor, for example, could bear responsibility for the alleged violation(s) and/or, for example, be required to defend and/or indemnify the business. On a related point, the business should also determine whether and when to reach out – likely through or at the direction of counsel – to any such vendor(s) to gather data and other information in furtherance of its investigation and defense.

9

The business should review its insurance policies, including, but not limited to, its cyber insurance policies, to determine whether any insurance coverage may be available for the claim. While many policies contain exclusions for TCPA or similar suits, some policies at least provide some limited coverage for defense costs.

10

The business should review its various consumer-facing agreements, terms, and conditions to determine whether the dispute is appropriate to be heard in court or must instead be arbitrated.

Leech Tishman's Insurance Coverage Group helps clients identify the coverages necessary for their businesses, review proposed policies and policy language, document and submit insurance claims if and when necessary, and negotiate with insurance companies to secure coverage.

Leech Tishman's Data Privacy & Cybersecurity Group counsels clients on preparing for and responding to data, privacy, and cybersecurity challenges. We offer clients a full spectrum of counseling and litigation capabilities, with a focus on privacy, data protection, information security, Internet and computer/cyber law, e-commerce, and consumer protection.