



TCPA Meets Cyber Data Breach Notification

FCC Seeks Comments on Banks' TCPA Exemption Request

By: Martin W. Jaszczuk, Molly McGinnis Stine, John F. Kloecker and Tamra J. Miller

Recent widespread and costly cyber data breaches have required or prompted affected organizations, including financial institutions, to quickly alert customers about possible account information compromises. But current statutes and regulations limit how organizations can make such notifications. A Catch-22 can result – compliance with data breach notification requirements can potentially be characterized as a violation of the Telephone Consumer Protection Act (TCPA).

Under the TCPA and its implementing regulations, calls or texts to cell phones using an automatic telephone dialing system (ATDS) or an artificial or prerecorded voice are illegal, except in emergencies or with the consent of the called party. See 47 U.S.C. § 227(b)(1)(A)(iii). However, the TCPA also allows the Federal Communications Commission (FCC), by rule or order, to exempt certain calls. See 47 U.S.C. § 227(b)(2)(C). See also *In the Matter of Cargo Airline Association Petition for Expedited Declaratory Ruling; Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991*, CG Docket No. 02-278, Order, 29 FCC Rcd 3432 (2014).

On October 14, 2014, the American Bankers Association (ABA) petitioned the FCC to request that certain time-sensitive calls and text messages be exempted. See *In the Matter of Petition for Exemption of the American Bankers Ass'n.*, CG Docket No. 02-278. The petition concerns calls alerting consumers to: (1) transactions and events that suggest a risk of fraud or identity theft; (2) possible breaches of the security of customers' personal information; (3) steps consumers can take to prevent or remedy harm caused by data security breaches; and (4) actions needed to arrange for receipt of pending money transfers.

The ABA asserts that such messages are "critical to financial institutions' efforts to prevent fraud and identity theft" or, in the case of money transfers, "facilitate time-sensitive consumer transactions and improve customer convenience." Such messages, according to the ABA, can be conveyed most efficiently and reliably through automated calls or texts to consumers' cell phones. Accordingly, the ABA seeks permission for its members to be allowed to send such messages without the prior express consent of the recipients.¹ The ABA proposes that it will work with telephone companies to ensure that such calls or texts are free to the users. The ABA also proposes other conditions for such messages, including that they be strictly confined to non-telemarketing information, only be sent to the telephone numbers of consumers to whom the alert is directed, identify the financial institution sending the messages, include the sender's contact information and reply instructions, be concise, and not be sent more often than necessary to complete the communications' intended purpose.



Furthermore, in the case of messages regarding money transfers, the ABA proposes that recipients of such messages will have the opportunity to opt-out of future communications.

The petition also notes that financial institutions face an array of data breach notification statutes and regulations. Section 501(b) of the Gramm-Leach-Bliley Act (15 U.S.C. § 6801) and related regulations require financial institutions to establish response and notification procedures for incidents involving unauthorized access to customers' personal information. In addition, at least 47 states and the District of Columbia have breach notification statutes that may subject financial institutions to similar or additional requirements. The ABA asserts that the requested exemption will facilitate compliance with these requirements and reduce the risk that such notifications would violate the TCPA.

The FCC has sought comment on the ABA's petition, with comments due December 8, 2014 and reply comments due December 22, 2014. The FCC's notice states that it "seek[s] comment on the issues raised in the Petition, including whether the exemptions requested in the Petition allow the financial services industry to reduce privacy and security risks proactively so that fraud, data security breaches, and identity theft are less likely to occur in the first place." The FCC also requests comment on whether it should consider additional or modified conditions to protect consumers from unwanted communications and from fraud, identity theft and data security breaches.

Should the FCC grant the ABA's petition, financial institutions will have bolstered their positions on two fronts. First, they will have additional support for making automated calls or texts about data breaches to customers' cell phones. Second, they will have additional support for stating that the FCC protects entities' use of such outreaches under the TCPA. We also note that if the ABA's petition succeeds with the FCC, other industries may pursue similar confirmation.

For a copy of the ABA Petition, [click here](#). For a copy of the FCC's Order seeking comments [click here](#).

¹ The ABA also notes in its petition that, while the FCC has noted that a customer who has provided a phone number to a financial institution has provided prior express consent to be contacted at that number unless he provides instructions to the contrary, a few courts have rejected the FCC's interpretation and have required additional evidence of prior express consent.

For more information on the matters discussed in this *Locke Lord QuickStudy*, please contact the authors:

Martin W. Jaszczuk | 312-443-0610 | mjaszczuk@lockelord.com

Molly McGinnis Stine | 312-443-0327 | mmstine@lockelord.com

John F. Kloecker | 312-443-0235 | jkloecker@lockelord.com

Tamra J. Miller | 312-443-1846 | tjmiller@lockelord.com