BEFORE THE
FEDERAL COMMUNICATIONS COMMISSION
WASHINGTON, D.C. 20554

In the Matter of	**)**	
	)	
Rules and Regulations Implementing the	**)**	**CG Docket No. 02-278**
Telephone Consumer Protection Act of 1991	**)**	
	)	**WC Docket No. 07-135**
American Bankers Association	**)**	
Petition for Exemption	**)**	

Electronic Transactions Association Comments
In Support Of The American Bankers Association's Petition For Reconsideration

The Electronic Transactions Association ("ETA"), through undersigned counsel, hereby submits these comments in support of the American Bankers Association ("ABA") Petition For Reconsideration and modification of the exemption from the Telephone Consumer Protection Act ("TCPA"), 47 U.S.C. § 227, that the Commission granted in the above-captioned proceeding in response to the ABA's Petition for Exemption for certain automated calls from financial institutions to mobile devices.[1] ETA is the leading trade association for the payments industry, representing over 500 companies that offer electronic transaction processing products and services. ETA's members include financial institutions that will be constrained in their efforts to inform customers of urgent situations regarding possible fraud, identity theft and data breaches by wireless call or text unless the provided-number condition is eliminated and replaced with a condition stating that exempted calls and texts may only be sent to customers

[1] *In the Matter of Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991, et al.*, CG Docket No. 02-278 and WC Docket No. 07-135, Declaratory Ruling and Order, FCC 15-72 (rel. July 10, 2015) ("Declaratory Ruling").

whose account or personal information is at risk and to money transfer recipients as requested by the ABA.

The Commission granted ABA's request for an exemption from the prior written consent requirement for financial institutions to send free-to-end-user, time sensitive voice and text messages to wireless devices to inform their customers of possible fraud or identity theft, data breaches and data breach remediation measures and to provide notice to money transfer recipients of the steps that must be taken to access the funds.[2] It conditioned the exemption, however, on the calls and text messages being sent "only to the wireless number provided by the customer of the financial institution."[3] As ABA persuasively demonstrates in its Petition, this condition effectively eviscerates the exemption and should be modified to provide that such calls and texts may only be sent to customers whose account or personal information is at risk and to money transfer recipients.[4]

The Commission has appropriately recognized that mobile wireless devices have become "an absolutely central part of Americans' daily lives."[5] Moreover, the number of Americans and American households cutting the wireline telephone cord to go wireless continues to increase. The most recent report from the Centers for Disease

---

2 Declaratory Ruling at ¶¶127-139.

3 *Id.* at ¶ 138.

4 ABA Petition at 5-8.

5 *In the Matter of Implementation of Section 6002(b) of the Omnibus Budget Reconciliation Act of 1993*, WT Docket No. 13-135, Seventeenth Report at 4, DA 14-1862 (rel. Dec. 18, 2014).

Control estimates that 106 million adults (44.1 percent of all adults) live in households with only wireless telephones.[6]

As the Commission is well aware, the personal information, including social security numbers[7] and debit and credit card data,[8] of tens of millions of Americans has been compromised in the last couple of years alone by security breaches that have taken place everywhere from the federal government, to health insurance companies and health care providers, to retail establishments.[9] Such personal information can be used to

---

[6] Centers for Disease Control and Prevention, Wireless Substitution: Early Release of Estimates from the National Health Interview Survey, July – December 2014 at 2 (June 2015). This represents a significant increase over the 39 percent wireless only households figure cited by the Commission for the second half of 2013. Declaratory Ruling at ¶ 7.

[7] *See e.g.*, Kaveh Waddell and Dustin Volz, "OPM Announces More Than 21 Million Affected by Second Data Breach," National Journal (July 9, 2015) (more than 22.1 million social security numbers compromised in the two breaches that occurred at the Office of Personnel Management), available at http://www.nationaljournal.com/tech/hack-opm-office-personnel-management-cyber-million-20150709

[8] Sarah Halzack, "Target Data Breach Victims Could Get Up to $10,000 Each From Court Settlement," Washington Post (March 19, 2015) (Target data breach exposed debit and credit card information for 40 million customer accounts), available at http://www.washingtonpost.com/news/business/wp/2015/03/19/target-data-breach-victims-could-get-up-10000-each-from-court-settlement/.

[9] See Kaveh Waddell and Dustin Volz, "OPM Announces More Than 21 Million Affected by Second Data Breach," National Journal (July 9, 2015) available at http://www.nationaljournal.com/tech/hack-opm-office-personnel-management-cyber-million-20150709; Michael Hiltzik, "Anthem is Warning Consumers about its Huge Data Breach. Here's a Translation," Los Angeles Times (March 6, 2015) (data breach affected 80 million Americans), available at http://www.latimes.com/business/hiltzik/la-fi-mh-anthem-is-warning-consumers-20150306-column.html; Steve Weisman, "Another Healthcare Data Breach," USA Today (July 25, 2015) (UCLA Health System data breach affected 4.5 million people) available at http://www.usatoday.com/story/money/personalfinance/2015/07/24/steve-weisman-health-care-data-breach/30593661/; Sarah Halzack, "Target Data Breach Victims Could Get Up to $10,000 Each From Court Settlement," Washington Post (March 19, 2015)

perpetrate crimes of fraud and identity theft. Now more than ever, consumers need and should have access to timely information on their wireless phones from their financial institutions about the security of their finances and personal information.

Text messaging can and does play a highly critical role in notifying consumers in real time of suspicious activity related to their accounts. According to data culled by CSID,[10] the most common sources of consumer fraud alerts are financial institutions and card providers and more than 1 in 10 victims discover that they are victims of fraud through a financial or fraud alert text.[11]

In granting ABA's request to exempt financial institutions from the prior express consent requirement for calls and texts intended to avert fraudulent transactions and identity theft and to notify consumers of data breaches, the Commission recognized that "a quick, timely communication with a consumer could prevent considerable consumer harms from occurring or . . . help mitigate the extent of harm that will occur."[12] Given the serious financial and other adverse consequences to which consumers may be exposed from fraud, identity theft and data breaches, alerting them to the possibility of suspicious activity as quickly as possible provides not only valuable assistance to the individual consumer but also to all of the other individuals and businesses that may be

---

available at http://www.washingtonpost.com/news/business/wp/2015/03/19/target-data-breach-victims-could-get-up-10000-each-from-court-settlement/.

[10] CSID provides identity protection and fraud detection services and technologies. https://www.csid.com/company/.

[11] See Data Breaches By Industry available at https://www.csid.com/resources/stats/data-breaches-by-industry/.

[12] Declaratory Ruling at ¶132.

negatively impacted by the fraud or data breach and a public service to the economy overall.

To preserve the efficacy of real time voice messages and text alerts made to consumers by financial institutions, the Commission should eliminate the condition that such calls and text messages may only be sent to the wireless number provided by the customer. Otherwise, customers whose account information does not contain a wireless phone number will not be able to receive real time fraud, identity theft and data breach alerts that may enable them to take action to thwart a crime before it is completed and serious damage is done.[13] The provided number condition will also prevent financial institutions from using voice calls or text messaging to notify the recipient of transferred funds what must be done to access the funds if the recipient does not have an account relationship with the sending institution[14] and even if the recipient does have such an account, only if the recipient has provided a wireless number to the financial institution. A financial institution could never meet the provided number condition for a non-customer that is the intended recipient of a money transfer. Thus, the very noble and consumer-friendly purposes that the Commission intended to achieve by exempting financial institutions from the express prior written consent requirement for certain wireless communications will be frustrated by the provided number condition.

---

13 ABA stated that one large bank reported that the provided number condition would stop 75 percent of the calls and texts it sends to alert customers to potential fraud on an account or data breach. ABA Petition for Reconsideration at 7.

14 In granting the exemption from the prior written consent requirement, the Commission cited the ABA's assertion that money transfers often must be sent to persons who do not have an ongoing relationship with the sending financial institution. Declaratory Ruling at ¶133.

ETA wholeheartedly agrees with ABA's discussion of the importance of allowing financial institutions to use any contact numbers they may have for their customers, whether or not provided directly by the customers, to convey fraud and identity theft alerts, data breach notifications and post-data breach mitigation notifications.[15] To the extent that financial institutions obtain wireless telephone numbers of customers from other financial institutions when accounts are transferred at the customer's direction, or from third party sources in the course of their USA PATRIOT Act investigations to confirm their customers' identities, or from other third party sources in the normal course of business, they should not be prohibited from using those numbers to provide urgent, time-sensitive information to their customers to prevent or mitigate financial and other harms that may result from fraud, identity theft and data breaches.

The conditions, other than the provided number condition, that the Commission has imposed on the exemption are more than sufficient to protect consumers and their privacy interests without compromising the ability of financial institutions to communicate exigent circumstances to customers in real time. Most significantly, one condition requires financial institutions to include in their messages a mechanism for recipients to easily opt out of receiving future calls and another requires the financial institutions to honor any opt-out requests immediately.[16] Yet another condition strictly limits the purposes for which voice calls and text messages may be sent and prohibits include any telemarketing, cross-marketing, solicitation, debt collection or advertising content in the calls and messages. Finally, the Commission has required that calls and

---

15 ABA Petition at 8-10.

16 Declaratory Ruling at ¶138.

text messages must be free to the consumer and cannot count against any limits on the consumer's voice or data plan.[17] These conditions will ensure (1) that customers retain the power and the right to stop receiving unwanted calls and texts from their financial institutions about potential fraud, identity theft or data breaches; (2) that voice calls and texts sent pursuant to the exemption do not subject consumers to the receipt of unwanted telemarketing, advertising, debt collection, or solicitation content; and (3) that consumers are not charged for calls and text messages to their wireless phones sent pursuant to the exemption.

For the foregoing reasons and those set forth in the ABA's Petition for Reconsideration, the Commission should grant ABA's Petition, eliminate the condition that calls and texts may only be sent to a wireless number provided by the customer of the financial institution and replace it with a condition that calls and texts may only be sent to customers whose accounts or personal information are at risk and to money transfer recipients.

August 17, 2015

Respectfully submitted,

Scott Talbott
Mary C. Albert
Electronic Transactions Association
1101 16th Street N.W., Suite 402
Washington, D.C. 20036
(202) 828-2635
stalbott@electran.org

[17] *Id.* at ¶¶ 138-139.