Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554

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

PETITION FOR EXEMPTION OF THE AMERICAN BANKERS ASSOCIATION

Virginia O'Neill
Vice President and Assistant
Chief Compliance Counsel
American Bankers Association
1120 Connecticut Avenue, N.W.
Washington, DC 20036
(202) 663-5073

Charles H. Kennedy
The Kennedy Privacy Law Firm
1050 30th Street, N.W.
Washington, DC 20007
(202) 250-3704

October 14, 2014

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The American Bankers Association requests that the Commission exercise its statutory authority to exempt certain time-sensitive informational calls, placed without charge to the called parties, from the Telephone Consumer Protection Act's restrictions on automated calls to mobile devices. The calls for which the exemption is requested would alert consumers concerning: (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. All of these messages serve consumers' interests and can be conveyed most efficiently and reliably by automated calls to consumers' telephones, which increasingly are wireless devices. Accordingly, the American Bankers Association requests an order that would permit financial institutions to send messages in these specific categories, using an automatic telephone dialing system or an artificial or prerecorded voice, without the recipient's prior express consent, on a free-to-end-user basis subject to such conditions as the Commission may prescribe as necessary in the interest of the privacy rights the Telephone Consumer Protection Act is intended to protect.

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554

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

PETITION FOR EXEMPTION OF THE AMERICAN BANKERS ASSOCIATION

The member banks of the American Bankers Association (ABA)[1] and other financial institutions must convey many types of non-marketing information to consumers in a prompt and effective manner. Some of these messages, such as data security breach notifications and verification calls to consumers who have placed fraud alerts on their credit reports, are required by law.[2] Others, such as notices of out-of-

[1] The American Bankers Association is the voice of the nation's $15 trillion banking industry, which is composed of small, regional and large banks that together employ more than 2 million people, safeguard $11 trillion in deposits and extend more than $8 trillion in loans.

ABA believes that government policies should recognize the industry's diversity. Laws and regulations should be tailored to correspond to a bank's charter, business model, geography and risk profile. This policymaking approach avoids the negative economic consequences of burdensome, unsuitable and inefficient bank regulation.

Through a broad array of information, training, staff expertise and resources, ABA supports banks as they perform their critical role as drivers of America's economic growth and job creation.

[2] *See* discussion at pp. 10, 11, 13, *infra.*

pattern account activity and transaction requests, are critical to financial institutions' efforts to prevent fraud and identity theft.[3] Finally, messages that advise money transfer recipients of how to claim transferred funds facilitate time-sensitive consumer transactions and improve customer convenience.[4]

ABA members strive to make these notifications quickly and efficiently. Financial institutions have found that automated communications are best suited to achieve these goals. Automated text messages are nearly instantaneous, and automatically-dialed voice calls and texts can reach more customers in any given period of time than manually-dialed calls.[5] In addition, automated text and voice message calls to mobile phones reach consumers wherever they are. Research shows that 98% of text messages are opened and most are read within three minutes of delivery, enabling consumers and financial institutions to react promptly to time-critical information and contain any potential damage that might be caused by a fraudulent transaction, data security breach, or other event.[6]

---

[3] *See* discussion at pp. 9, 12, *infra.*

[4] *See* discussion at pp. 15, 16, *infra.*

[5] One ABA member reports that when calls to customers are placed manually by a live operator, only 34% of those calls reach the intended party on the first attempt. By contrast, automated live-operator calls reach the intended party on 61% of first attempts, and the number of calls an employee can place by automated means over any given time exceeds the number of calls the employee can place manually by 281.6%. When time-critical messages must be delivered to thousands of customers within a short time, these differences in completion rates have significant consequences for those customers' interests.

[6] Aine Doherty, *SMS Versus Email Marketing*, business2community.com (July 28, 2014), available at http://www.business2community.com/digital-marketing/sms-versus-email-marketing-0957139#!bth7SG (*Doherty*); Cheryl Conner, *Fifty Essential Mobile Marketing Facts*, FORBES.COM (Nov. 12, 2013), *available at* http://www.forbes.com/sites/cherylsnappconner/2013/11/12/fifty-essential-mobile-marketing-facts. In contrast to the 98% success rate of text messaging, only 22% of email messages are opened. *Doherty*, *supra.*

A substantial percentage of these automated notifications *must* be sent to mobile telephone numbers. One ABA member bank reports that approximately half of its account holders have mobile telephone numbers, and approximately 25% of its account holders subscribe to mobile telephone service but do not subscribe to landline telephone service. These statistics are consistent with those contained in recent reports by CTIA – The Wireless Association (CTIA) and the Centers for Disease Control (CDC). Specifically, CTIA reports that as of year-end 2013, 39.4% of U.S. households were "wireless only;" and CDC reports that 41% of U.S. households were "wireless only," with that percentage rising to 65.7% for adults between the ages of 25 and 29.[7] These percentages have increased steadily for many years, so that any impediment to automated contact with mobile customers facing risk of fraud or identity theft is likely to affect more than half of financial institution customers in coming years.

Moreover, consumers increasingly prefer that their financial institutions use all available channels to advise them of potential fraud or other time-sensitive events. A 2010 survey conducted for SoundBite Communications Inc. showed that nearly 60 percent of consumers preferred to be contacted on their mobile telephones concerning potentially fraudulent activity, and that more than one in three consumers preferred to

[7] CTIA Annual Wireless Industry Survey, *available at* http://www.ctia.org/your-wireless-life/how-wireless-works/annual-wireless-industry-surveyhtm; Stephen J. Blumberg and Julian V. Luke, *Wireless Substitution: Early Release of Estimates from the National Health Interview Survey, July – December 2013, available at* http://www.cdc.gov/nchs/nhis.htm; Karen Kaplan, *Still Have a Landline? 128 Million Don't,*LOS ANGELES TIMES (July 8, 2014).

receive those notifications by means of text messaging. The survey showed that these efficient communications channels are used far less often than consumers would prefer.[8]

However, the ongoing flood of TCPA class action law suits, alleging that automated calls were placed to mobile devices without the recipients' prior express consent, has severely hampered the willingness and ability of financial institutions to reach consumers' mobile devices by automated means.[9] Even when a customer has furnished a mobile telephone number to the institution making the automated call, plaintiffs' attorneys may assert that the consumer providing the number did not specifically consent to receive fraud and identity theft alerts.[10] For this reason, financial institutions that attempt to reach customers in the most timely and reliable fashion may be forced to defend class action suits alleging that they violated the TCPA by sending automated

---

[8] *A Phone Call Isn't Enough: New Survey Shows 89 Percent of Consumers Want Fraud Communication Via Multiple Channels, available at* http://www.harrisinteractive.com/vault/client_news_soundbite_2010_04.pdf.

[9] *See* U.S. Chamber of Commerce Institute for Legal Reform, *The Juggernaut of TCPA Litigation* (Oct. 2013).

[10] ABA agrees with this Commission's finding that "persons who knowingly release their phone numbers have in effect given their invitation or permission to be called at the number which they have given, absent instructions to the contrary." *See Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991*, 7 FCC Rcd 8752, 8769 (1992); *see also Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991; Request of ACA International for Clarification and Declaratory Ruling*, 23 FCC Rcd 559, 564 (2008). Accordingly, ABA continues to take the position that when customers of its member banks provide mobile contact numbers in the course of a transaction or account relationship, the bank has obtained prior express consent to call that number by automated means in the course of the relationship. However, some courts have rejected the Commission's interpretation of the prior express consent requirement, thereby creating a risk that TCPA class-action plaintiffs will defeat defenses based on such consent. *See, e.g., Mais v. Gulf Cost Collection Bureau, Inc.*, Case No. 11-61936-CIV, 2013 WL 1899616 (S.D. Fla. 2013), *reversed and remanded*, No. 13-14008, 2014 U.S. App. LEXIS 18554 at *3-12 (11th Cir. 2014); *see also Leckler v. Cashcall, Inc.*, 554 F.Supp.2d 1025 (N.D. Cal. 2008), *vacated by Leckler v. Cashcall, Inc.*, 2008 WL 5000528 (N.D. Cal. 2008). By granting ABA's request for exemption, the FCC will reduce or remove this risk with no harm to consumers.

messages to mobile devices without the recipients' prior express consent. One ABA member reports that because of the legal risks posed by TCPA class-action litigation, only 40% of the merchant data security breach notification alerts that might be sent to customers by automated means are sent.

As many commenters and petitioners in this docket have pointed out, interpretation of the TCPA in accordance with its plain language and intent would remove this artificial obstacle to efficient customer communications.[11] Notably, the dialing systems used by responsible businesses seeking to provide informational messages to customers do not have the present capacity to store or produce numbers to be called using a random or sequential number generator, and to dial such numbers, and therefore do not fit the TCPA's definition of an automatic telephone dialing system (ATDS).[12] A declaration or clarification by this Commission that simply acknowledged the ATDS definition's plain meaning would provide authoritative guidance to the courts and relieve callers from the unreasonable and excessive litigation risks they now face. As Commissioner O'Rielly has pointed out, the FCC should "follow through on the pending TCPA petitions to make sure that good actors and innovators are not needlessly subjected to enforcement actions or lawsuits, which could discourage them from offering new consumer-friendly communications services."[13]

---

[11] *See, e.g.,* Petition for Declaratory Ruling of Communication Innovators, CG Docket No. 02-278 (filed June 7, 2012); Petition for Expedited Declaratory Ruling of YouMail, Inc., CG Docket No. 02-278 (filed April 19, 2013); Petition of Glide Talk, Ltd. for Expedited Declaratory Ruling, CG Docket No. 02-278 (filed Oct. 28, 2013); Petition for Rulemaking of ACA International, CG Docket No. 02-278 (filed Jan. 31, 2014).
[12] 47 U.S.C. § 227(a)(1).
[13] Michael O'Rielly, *TCPA: It is Time to Provide Clarity*, OFFICIAL FCC BLOG (Mar. 25, 2014), *available at* http:www.fcc.gov/blog/tcpa-it-time-provide-clarity.

ABA continues to support petitions pending before this Commission that seek declaratory relief concerning the application of the TCPA's autodialer restriction, including those petitions that seek clarification of the ATDS definition.[14] However, and without conceding that the autodialer restriction applies to the informational communications described here, this petition asks the Commission to exempt certain categories of consumer communications from that restriction to the extent they are sent without charge to the called party, subject to such reasonable conditions as the Commission may impose, under the process authorized by 47 U.S. Code section 227(b)(2)(C) and utilized by the Commission in its recent Order granting an exemption from the autodialer restriction for package delivery notifications.[15] The following more fully describes the categories of communications for which ABA seeks exemption, and the reasons why such exemptions are necessary and in the public interest.

I. MESSAGES REQUIRED TO PROTECT CONSUMERS FROM FRAUD AND IDENTIFY THEFT

Identity theft and fraud losses are at historically high levels. Javelin Strategy & Research reports an increase of more than 500,000 fraud victims in 2013, bringing the total for the year to 13.1 million people. Encouragingly, the amount criminals stole

[14] *See* Comments of the American Bankers Association in support of ACA International Petition for Rulemaking, CG Docket No. 02-278 (filed March 24, 2014); Reply Comments of the American Bankers Association in support of Petition of Retail Industry Leaders for Declaratory Ruling, CG Docket No. 02-278 (filed March 10, 2014).
[15] 47 U.S.C. § 227(b)(2)(C); *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 released March 27, 2014) (*"CAA Order"*).

decreased by $3 billion to $18 billion in 2013, reflecting more aggressive actions by financial institutions and consumers to combat fraud and identity theft. [16]

Protecting customers from fraud and identity theft is a high priority of the financial services industry. Financial institutions have made significant investments in fraud monitoring to identify suspicious activities and transactions and to respond with timely messages to customers that might be at risk. Among the activities and risk factors financial institutions monitor for these purposes are:

- Customer purchases that are unusual in kind for the customer, such as purchases in amounts, in geographic areas, or at types of merchant that depart from the customer's established buying patterns.
- Transaction authorization requests that present a high likelihood of fraud, such as high-dollar transactions, ATM withdrawals, and purchases of goods that can readily be converted to cash.
- Transaction requests involving geographic areas, merchants, or merchant types that recently have experienced unusual levels of fraud.
- Suspicious non-monetary activities, such as changes of address closely accompanied by requests for new payment cards.[17]

---

[16] Javelin Strategy & Research, *A New Identity Fraud Victim Every Two Seconds in 2013 According to Latest Javelin Strategy & Research Study*, February 5, 2014, *available at* https://www.javelinstrategy.com/news/1467/92/A-New-Identity-Fraud-Victim-Every-Two-Seconds-in-2013-According-to-Latest-Javelin-Strategy-Research-Study/d,pressRoomDetail.

[17] The Red Flags Rule, adopted by the Federal Trade Commission and other federal regulators of financial institutions, prohibits a card issuer from complying with a request for an additional or replacement card that follows less than 30 days after an address change, until it has notified the cardholder of the request. *See, e.g.*, 16 C.F.R. § 681.3.

- Requests for new online credentials, coupled with evidence of malware or phishing attacks.

Financial institutions do not alert customers each time one of these activities is detected. Instead, those institutions use experience-based algorithms to identify those events that present an increased risk of fraud or identity theft. However, when financial institutions identify potentially suspicious activities that satisfy these algorithms, effective fraud prevention requires the earliest possible contact with the customer. The volume of these notifications, which average 300,000 to 400,000 messages per month for one ABA member alone, cannot be accomplished with acceptable speed and accuracy unless the process is automated.[18] Manual calls placed in these circumstances would come too late to prevent harm or inconvenience to the customer, and may not even be attempted because of the sheer impracticality of the undertaking.

In addition, financial institutions are required under the Fair Credit Reporting Act to verify a customer's identity before authorizing the establishment of any new credit plan or extension of credit where a fraud alert has been placed on the customer's credit reporting agency file.[19] Financial institutions rely on the efficiency of autodialers and other automation technologies to contact these customers quickly, with the goal of verifying identity and immediately accommodating the customer's request. For those customers who can most efficiently be contacted at mobile telephone numbers, the

---

[18] *See* Quantria Strategies, LLC, *Modifying the TCPA to Improve Services to Student Loan Borrowers and Enhance Performance of Federal Loan Portfolios*, July 2013, p. 9, *available at* http://apps.fcc.gov/ecfs/document/view?id=7521337606 (reporting a gain in efficiency of 281.6% when student loan servicers used predictive dialers as opposed to manual dialing).

[19] Fair Credit Reporting Act § 605A, 15 U.S.C. § 1681c-1.

inability to use automated calling methods is likely to delay the bank's ability to contact the customer, resulting in embarrassment — or worse — for those customers. ABA regards these verification calls as part of its members' fraud and identity theft prevention efforts, and therefore asks that the proposed exemption apply to such calls.

Given these realities, fraud and identity theft alerts are ideally suited to relief under the exemption procedure of TCPA section 227(b)(2)(C).

II. DATA SECURITY BREACH NOTIFICATIONS

Breaches of the security of personal information are perhaps the most important, and the fastest-growing, privacy issue facing consumers today. Since January 2005, a total of over 4,816 breaches exposing more than 667 million consumer records have occurred nationwide. There were over 600 reported data breaches during 2013, an increase of 30 percent over 2012, and the third highest number of breaches over the last nine years. To date in 2014, 368 data breaches have been reported.[20] Notably, the breach of customers' personal information, payment card data and encrypted PIN numbers at Target affected over 70 million customers; malware placed on Home Depot's point-of-sale credit card readers affected at least 56 million customers; a data breach at the California Department of Motor Vehicles exposed data concerning 11.9 million payment card transactions; and a breach at the University of Maryland exposed personal information of at least 300,000 students and employees. In fact, almost half of American adults (47%) had their personal information exposed by hackers between August of 2013

[20] Identity Theft Resource Center, June 5, 2014, *available at* http://www.idtheftcenter.org/id-theft/data-breaches.html.

and August 2014, and 41% of adult Americans have had to replace at least one credit card for fraud prevention reasons so far in 2014.[21]

Section 501(b) of the Gramm-Leach-Bliley Act, as well as the data security breach notification statutes of 47 states and the District of Columbia, require financial institutions and other organizations to establish response and customer notification programs following any unauthorized access to customers' personal information that is maintained by those organizations.[22] Besides complying with their legal obligation to report breaches of customer data that they maintain, financial institutions protect their customers by alerting them to data breaches, at retailers and other businesses, that threaten the security of those customers' financial account information.[23] Accordingly, upon learning of any data breach at a merchant or other organization that potentially affects an institution's customers, the financial institution immediately seeks to contact its customers to notify them of the breach and of any remedial action to be taken.[24]As a

---

[21] Jose Pagliery, *Welcome to the Age of Hacks*, CNN MONEY (Sept. 4, 2014), available at http://money.cnn.com/2014/09/04/technology/security/age-of-the-hack/index.html.

[22] Gramm-Leach-Bliley Financial Services Modernization Act of 1999, Pub. L. No. 106-102, 113 Stat. 1338, § 501(b); *see, e.g.*, Cal. Civ. Code § 1798.29; Fla. Stat. § 817.5681; 815 ILCS § 530/10(a); NY CLS Gen. Bus. § 899aa; N.C. Gen. Stat. § 75-65; Rev. Code Wash. § 19.255.010.

[23] Testimony before the California State Senate in February, 2014 confirmed that consumers often receive notice of retailer data security breaches affecting payment card information from their banks rather than from the affected retailers. Joint Hearing of Senate Banking and Financial Institutions Committee and Senate Judiciary Committee, *Beyond the Breach: Protecting Consumers' Personal Information in the Retail Environment* (Feb. 25, 2014); video of hearing available at http://senate.ca.gov/vod/20140225_1317_STV1Vid.

[24] As a result, our payment system remains strong and functional. No security breach has deterred the $3 trillion that Americans spend safely and securely each year with their credit and debit cards, confident that their financial institution has invested in technology to detect and prevent fraud. ABA and the thousands of community, mid-size, regional, and large banks it represents recognize the paramount importance of a safe and secure payments system to our nation and its citizens.

result, even though their industry is a source of only a small percentage of data security breaches, financial institutions deal in a high volume of data security breach notifications.[25] A single financial institution might be responsible for 50,000 to 60,000 or more potential data security breach notifications per month.

Breach notification messages present the same issues as fraud and identity theft alerts and support a similarly compelling case for exemption from the TCPA's prior express consent requirements. Like fraud and identity theft alerts, breach notification alerts must be timely and reliable. As with fraud and identity theft alerts, breach notification messages might have to be sent to mobile numbers that were not provided directly by the recipient, and even sending automated messages to customer-provided mobile numbers presents a substantial risk of legal liability because of potential class-action plaintiffs' claims that those consents are inadequate. Accordingly, ABA requests that the proposed exemption under TCPA section 227(b)(2)(C) apply to notices of suspected breaches in the security of consumers' personal information.

III. REMEDIATION MESSAGES

Closely related to data security breach notification messages are notices to customers concerning measures they may take to prevent identity theft resulting from a breach, such as placing fraud alerts on their credit reports and subscribing to credit monitoring services. Remediation messages also include notices to customers that they will be

---

[25] The banking, credit, and financial industry accounted for only 3.7% of data breaches reported between 2005 and 2013. The two sectors of the economy reporting the highest number of breaches during that time were the healthcare sector at 43% and the business sector, including merchants, at almost 34%. *See* http://www.idtheftcenter.org/images/breach/20052013UPDATEDSummary.jpg.

receiving new payment cards, how to activate those cards, and how to take other steps that will ensure the availability of secure card transactions. Following many notable security breaches, affected institutions have offered to provide such services for consumers at no charge to the consumer. The volume and frequency of these remediation notices equal those of the original breach notification messages and present a similar case for exemption from TCPA prior express consent requirements. Accordingly, the ABA requests that those messages be included in the proposed exemption.

IV. MONEY TRANSFER NOTIFICATIONS

Mobile money transfers are an increasingly popular means of making rapid transfers from one consumer's account to another consumer's account. Because of the efficiency and ubiquity of text messaging, senders of money transfers often prefer that their financial institutions send a text, notifying recipients of the steps to be taken in order to obtain the transferred funds. Senders also may prefer to receive a receipt for their money transfers (as required by state money transfer laws) in real time and through the same channel from which the transfers are initiated.

These notification texts present essentially the same issue as the package delivery notifications that were the subject of the Cargo Airline Association's request for a TCPA exemption.[26] Like package delivery notifications, money transfer notifications are welcomed by their recipients, but often must be delivered to persons who do not have an ongoing relationship with the sending institution and therefore have not consented to receive automated calls from that institution. Obtaining consent from recipients in these circumstances would be impractical and burdensome and would not serve consumers'

[26] *CAA Order, supra.*

interests. Delays incurred to obtain consent also might be inconsistent with state money transfer laws that require those transfers to be completed promptly.[27] Accordingly, ABA requests that these money transfer notification messages should be exempted from TCPA prior express consent requirements to the extent they are sent on a free-to-end-user basis.

V. PROPOSED CONDITIONS

As the Commission pointed out in its recent *CAA Order*, TCPA section 227(b)(2)(C) "authorizes the Commission 'by rule or order' to exempt, from the restriction on autodialed and prerecorded calls and messages to wireless telephone numbers, such calls and messages 'that are not charged to the called party, subject to such conditions as the Commission may prescribe as necessary in the interest of the privacy rights the provision is intended to protect.'"[28] The *CAA Order,* which represents the Commission's first use of its authority under section 227(b)(2)(C), granted an exemption for a narrowly-defined category of informational messages that the Commission found would benefit consumers without burdening those consumers' privacy interests under the TCPA. In order to ensure the protection of those privacy interests, the Commission conditioned the exemption on the petitioner's compliance with seven conditions.

This petition requests relief similar to that granted in the *CAA Order.* ABA proposes an exemption that will permit financial institutions to send automated fraud and identity theft alerts, security breach notifications, remediation messages, and money transfer notices with content confined strictly to non-telemarketing information, to customers on a free-to-end-user basis, subject to such reasonable conditions as the Commission may

[27] *See, e.g.,* Cal. Fin. Code § 2102.
[28] *CAA Order* ¶ 7.

prescribe as necessary to protect the privacy rights the TCPA is intended to serve. Like Cargo Airline Association, financial institutions will work with wireless carriers and third-party service providers to ensure that recipients of notices under the requested exemption are not charged for those messages. ABA further acknowledges, as the Commission pointed out in its *CAA Order*, that any exemption granted will not extend to "notifications that count against the recipient's plan minutes or texts."[29]

ABA also proposes to observe the following conditions, which correspond to those specified in the *CAA Order*, when sending messages subject to the proposed exemption:

1. Automated messages subject to the exemption will be sent only to the telephone numbers of consumers to whom the alert is directed.

In the case of fraud/identity theft, data security breach, and remediation messages, automated alert messages will be sent to the telephone numbers of financial institution customers whose accounts or personal information is at risk. In the case of money transfer notices, messages will be sent only to the designated recipients of transferred funds.[30]

[29] *CAA Order* ¶ 12.

[30] As petitions and filings pending before the Commission have pointed out, even the best compliance measures cannot entirely prevent calls from being answered by persons to whom they are not directed — for example, where a mobile telephone number has been reassigned without the caller's knowledge. Petition for Declaratory Ruling of the Consumer Bankers Association (Sept. 19, 2014); Letter from Monica S. Desai to Marlene H. Dortch (July 21, 2014); Letter from Monica S. Desai to Marlene H. Dortch (May 15, 2014); Rubio's Restaurant, Inc. Petition for Expedited Declaratory Ruling (Aug. 11, 2014); Petition for Expedited Declaratory Ruling of United Healthcare Services, Inc. (Jan. 16, 2014), all in CG Docket No. 02-278. ABA agrees with these petitioners that callers should not be liable for such calls under the TCPA, and urges the Commission to grant the relief these petitioners have requested.

2. **Automated messages subject to the exemption will identify the name of the financial institution sending those messages and will include the sender's contact information or reply instructions.**

3. **Automated messages subject to the exemption will not contain any telemarketing, solicitation or advertising content.**

4. **Automated messages subject to the exemption will be concise, generally one minute or less in length for voice calls unless more time is needed to obtain customer responses or answer customer questions, and no more than 160 characters in length for text messages.**

5. **Financial institutions will send no more automated messages than are required to complete the communications' intended purpose.**

As the Commission recognized in its *CAA Order* a single message is not always sufficient to serve the purpose for which an organization might need to contact a consumer. Accordingly, the exemption granted to Cargo Airline Association permitted more than one package delivery notice to be sent if required to obtain a recipient's signature.[31] Some of the information that will be conveyed to consumers pursuant to the exemption requested in this petition will require more than one automated voice call or text message.

Indeed, with regard to data security breach notification messages, fraud and identity theft alerts, and remediation messages, the Commission will *protect* consumers if it does not to impose arbitrary limitations on the number of automated fraud-related calls or texts that may be sent. Moreover, financial institutions have no incentive to send an excessive number of these messages, and in practice, it is the consumer that controls the number and nature of the messages exchanged.

[31] *CAA Order*, ¶ 15.

For example, to combat fraud and identity theft financial institutions seek to alert customers to potentially suspicious activity and to data security breaches. Consumers must be given a reasonable opportunity to respond to those messages, whether by authorizing the suspect transaction, by advising the financial institution that the transaction was not authorized, or by taking other action to protect the consumer's account. When consumers fail to respond to identity theft or breach notifications, financial institutions send follow-up messages. The period of time during which such communications will be attempted, however, is limited by the need to take prompt action to protect the consumer. ABA members report that they typically will make no more than three attempts per day and will cease trying to contact the consumer after two or, in the case of some financial institutions, three days.[32]

Accordingly, ABA requests that the exemption for breach and fraud-related communications should permit three such messages to be sent for a maximum of three days, if the consumer fails to respond. ABA also notes that three such messages per day for three days should be permitted for each affected account and for each affected co-borrower or co-cardholder.

ABA also requests that financial institutions be permitted to send communications, related to fraud and identity theft prevention, as required to respond to a customer message or otherwise complete the fraud-prevention process. For example, an automated notice of an out-of-pattern transaction will ask the consumer to respond (for example, by pressing "1" or "2") as to whether the consumer authorized the transaction.

[32] Following unsuccessful attempts to reach consumers by automated call or text, financial institutions resort to email and/or a letter.

When the financial institution receives the consumer's response, it will send an additional message, either telling the consumer that the transaction has been approved, or advising the consumer that the transaction was disallowed and explaining further steps he or she should take. If the transaction involves a payment card and the financial institution will be sending the consumer a new card, a further message might be sent, advising the customer that the card is coming and explaining how the card may be activated. All of these communications are essential steps in the consumer protection process.

Similarly, data security breach notification and remediation communications may require financial institutions to send more than one message. Notably, a data breach, like a suspicious transaction, might require a financial institution to explain to the customer how he or she can obtain a replacement payment card. For this reason, ABA requests that financial institutions be permitted, pursuant to the proposed exemption, to send as many messages as are needed to complete the process of breach notification and remediation and to respond to consumer messages that are part of that process.

With regard to a notice of a mobile money transfer, one automated message informing the consumer of the transfer is sufficient to complete the communications' intended purpose. Financial institutions will agree to a condition that permits only one automated, free-to-end-user notice of a mobile money transfer.

6. Recipients of money transfer notifications will have the opportunity to opt out of future such communications.

In its *CAA Order*, the Commission required package delivery companies to give package recipients the opportunity to opt out of receiving future automated delivery

notices.[33] Given that those notices were neither required by law, nor directly related to prevention of fraud or identity theft, the opt-out requirement was an appropriate limitation on the relief granted in that case.

In the present petition, ABA proposes an opt-out requirement for automated money transfer notices. However, ABA does not believe that such a limitation is appropriate for alerts related to fraud and identity theft, including remediation messages. If a customer should opt out of receiving those critical messages by automated means, the result will be that the same messages will be sent through channels that are less efficient and less likely to permit timely remedial action. ABA does not believe that this result is in the interests of consumers, and requests that the opt-out opportunity be limited to money transfer messages.

CONCLUSION

This petition for exemption identifies a specific set of non-telemarketing messages that are particularly appropriate for sending to consumers without a requirement of prior express consent, to the extent they are sent without charge to the recipient. The limited relief requested in this petition will permit the ABA's members and

[33] *CAA Order*, ¶ 16.

other financial institutions to serve their customers in a manner consistent with the public-service mandate of the Commission, and ABA requests that its petition be given prompt consideration.

Respectfully submitted,

//Virginia O'Neill

Virginia O'Neill
Vice President and Assistant
Chief Compliance Counsel
American Bankers Association
1120 Connecticut Avenue, N.W.
Washington, DC 20036
(202) 663-5073

//Charles H. Kennedy

Charles H. Kennedy
The Kennedy Privacy Law Firm
1050 30th Street, N.W.
Washington, DC 20007
(202) 250-3704

October 14, 2014