

**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 Telephone Consumer Protection Act of 1991)	CG Docket No. 02-278
)	

REPLY COMMENTS 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

December 19, 2014

TABLE OF CONTENTS

EXECUTIVE SUMMARY	3
I. THE PETITION IS SUPPORTED BY COMMENTERS REPRESENTING A WIDE RANGE OF INDUSTRIES AND INTERESTS	6
II. COMMENTERS AGREE THAT THE PROPOSED RELIEF WILL REDUCE PRIVACY AND SECURITY RISKS	10
III. THE COMMENTS CONFIRM THAT THE LITIGATION THREAT INHIBITS CRITICAL CUSTOMER COMMUNICATIONS	12
IV. THE COMMENTS DO NOT SUPPORT THE IMPOSITION OF ADDITIONAL CONDITIONS	14
CONCLUSION	16

EXECUTIVE SUMMARY

The comments filed in this proceeding show overwhelming support for the pending Petition for Exemption of the American Bankers Association. Proponents of granting the Petition include companies and associations in a wide range of industries and, perhaps most importantly, organizations devoted to the promotion of consumer privacy. No consumer rights or privacy rights organization filed in opposition to the Petition.

The comments also give overwhelmingly positive responses to the Commission's query, in the Public Notice, whether granting the requested relief would prevent fraud, data security breaches and identity theft from occurring in the first place; and most comments agree that the conditions proposed in the Petition will be sufficient to protect the interests the Telephone Consumer Protection Act is intended to advance. Commenters also confirm that the threat of ill-founded litigation is at present an impediment to the sending of messages that prevent and control harm to consumers.

Accordingly, 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 rather than landline devices.

**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 Telephone Consumer Protection Act of 1991)	CG Docket No. 02-278
)	

REPLY COMMENTS OF THE AMERICAN BANKERS ASSOCIATION

The comments filed in this proceeding overwhelmingly support the Petition for Exemption (Petition) of the American Bankers Association (ABA).¹ Commenters supporting the Petition represent a broad range of industries and interests, and consistently agree that by granting the Petition, the Commission will reduce the number of fraud and identity theft incidents that harm consumers, financial institutions, and the infrastructure of services that support and facilitate financial transactions. Accordingly, the record in this proceeding amply supports the granting of an exemption under section 227(b)(2)(C) of the Communications Act for automated fraud prevention, breach

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.

notification, remediation and money transfer notifications, sent to consumers' mobile devices on a free-to-end-user basis, subject to the conditions proposed in the Petition.

I. THE PETITION IS SUPPORTED BY COMMENTERS REPRESENTING A WIDE RANGE OF INDUSTRIES AND INTERESTS

Support for the Petition comes not only from financial institutions,² but from Internet technology companies,³ equipment and service vendors,⁴ payments processing networks⁵ and consumer privacy and fraud prevention organizations.⁶

² Letter from Brandon Kelly, FirstBank, to Federal Communications Commission (filed Dec. 8, 2014) (“FirstBank Comments”); Letter from Jennifer Martin, SAFE Credit Union, to Federal Communications Commission (filed Dec. 7, 2014) (“SAFE Comments”); Letter from Ann Wallace, Financial Services Roundtable, to Marlene H. Dortch) (filed Dec. 8, 2014) (“FSR Comments”); Comments of the Consumer Bankers Association (filed Dec. 8, 2014) (“CBA Comments”); Letter from Christopher L. Williamson, Independent Bankers Association of Texas, to Christina Clearwater (filed Dec. 8, 2014) (“IBAT Comments”); Letter from Patrick S. Jury, Iowa Credit Union League, to Federal Communications Commission (filed Dec. 8, 2014) (“ICUL Comments”); Letter from Bill Himpler, American Financial Services Association, to Federal Communications Commission (filed Dec. 8, 2014) (“AFSA Comments”); Letter from Diana R. Dykstra, California and Nevada Credit Union Leagues to Federal Communications Commission (filed Dec. 8, 2014) (“California and Nevada Credit Union Comments”); Comments of the Credit Union National Association in Support of Petition for Exemption of the American Bankers Association (filed Dec. 8, 2014) (“CUNA Comments”); Letter from Dennis E. Nixon, International Bancshares Corporation, to Christine Clearwater (filed Dec. 8, 2014) (“IBC Comments”); all in CG Docket No. 02-278.

³ Comments of the Internet Association (filed Dec. 8, 2014), CG Docket No. 02-278 (“IA Comments”).

⁴ Comments of Noble Systems Corporation (filed Dec. 8, 2014) (“Noble Systems Comments”); Letter from Steven A. Salzer, PSCU to Marlene H. Dortch (filed Dec. 8, 2014) (“PSCU Comments”); both in CG Docket No. 02-278.

⁵ Comments of MasterCard Incorporated in Support of the Petition for Exemption of the American Bankers Association (filed Dec. 8, 2014) (“MasterCard Comments”); Letter from Ky Tran-Trong, Visa, Inc. to Federal Communications Commission (filed Dec. 8, 2014) (“Visa Comments”); both in CG Docket No. 02-278.

⁶ Comments of the Future of Privacy Forum (filed Dec. 8, 2014) (“FPF Comments”); Comments of the Identity Theft Council (filed Dec. 8, 2014) (“ITC Comments”); Letter from Craig D. Spiezle, Online Trust Alliance (filed Dec. 8, 2014) (“OTA Comments”); all in CG Docket No. 02-278.

The privacy organizations make clear that by granting the Petition, the Commission not only will promote “the privacy rights [the TCPA] is intended to protect,” but will help to control the severe threats to consumer privacy posed by fraud and identity theft. As the Future of Privacy Forum points out, “[f]ree-to-end-user fraud and identity theft alerts, data breach notifications, remediation notices, and money transfer notifications will benefit consumer privacy and security by helping to prevent the dissemination of consumers’ personal financial and other private information.”⁷ Similarly, the Identity Theft Council points out that “with growing concern that personal emails and calls to landlines may be nothing more than elaborate phishing schemes, the mobile channel has become even more important as the consumer’s early warning system.”⁸ Finally, the Online Trust Alliance states that granting the Petition “will facilitate prompt and efficient communication of time-sensitive information that can both limit the occurrence and impact of online crime and identity theft.”⁹

Significantly, not a single privacy advocacy group or consumer protection organization filed in opposition to the Petition.

The Internet Association, representing major Internet-based companies such as Amazon, AOL, Facebook and Twitter, confirms the need from that industry’s perspective for increased use of automated messaging as a means of preventing fraud and identity theft. As the Internet Association points out, online services, no less than financial institutions, collect and maintain users’ personal information and are subject to account takeover attacks that result in theft of access credentials, payment card information and

⁷ FPF Comments at 10.

⁸ ITC Comments at 1.

⁹ OTA Comments at 2.

other data that can be misused to commit fraud and identity theft.¹⁰ The Internet Alliance strongly agrees with ABA that entities affected by suspicious activity “should be permitted to reach the affected customers in the most efficient and timely manner — via their mobile phones.”¹¹ The Internet Alliance also agrees that prompt notification of money transfers by automated messaging “may be critical to avoiding default, preventing overdraft, or ensuring receipt of funds by the correct party.”¹²

Another perspective is provided by MasterCard and Visa, which operate processing networks that coordinate payment card transactions among financial institutions that issue cards and the acquiring institutions that enter into payment card contracts with merchants. MasterCard emphasizes that all of the participants in the payment card system, including merchants and customers as well issuing and acquiring financial institutions, are affected by security incidents and unauthorized transactions:

[T]he safe operation of the payment network depends on the avoidance of fraudulent transactions being processed. Fraudulent transactions can result in a negative impact on cardholders and merchants and may lead to consumers’ being less willing to undertake and merchants less willing to accept payment card transactions that are processed over the MasterCard network. In addition, if there is an increase in fraudulent charges, the processing of disputes and reversals of those charges imposes additional demands on our network.¹³

¹⁰ IA Comments at 4-7.

¹¹ IA Comments at 7.

¹² IA Comments at 4-8. ABA takes no position on the Internet Association’s request that “the FCC exemption allow entities in any industry (including the Internet industry) to notify users, via SMS or call, of a suspected takeover or other account security alert” or of a data security breach. *Id.* at 5-7. However, to the extent the Internet Alliance’s request would require consideration of matters not in the present record, or the filing of a separate petition for exemption, ABA urges the Commission not to delay its disposition of the ABA Petition because of the Internet Association’s request.

¹³ MasterCard Comments at 3. Similarly, Visa states that its support for the Petition is based on its “strong interest in protecting cardholders and the integrity of the electronic payments system and ensuring that the use of payment cards and payment card

Visa and MasterCard agree that these harms can most effectively be avoided if financial institutions are allowed to send fraud alert, breach notification, remediation and money transfer messages to consumers' mobile devices by automated means.

The supporting comments from financial institutions also represent a variety of perspectives. Notably, many comments were filed by local community banks, credit unions, and their state association representatives. For example, the Independent Bankers Association of Texas represents “over 400 independent community banks domiciled in Texas”;¹⁴ the California and Nevada Credit Union Leagues speak for “nearly 400 credit unions and their 10 million member customers”;¹⁵ SAFE Credit Union serves customers in twelve California counties;¹⁶ the Iowa Credit Union League represents Iowa's 109 credit unions;¹⁷ and the Credit Union National Association represents 6,700 state and federal credit unions serving over 100 million members.¹⁸ These comments underscore the diversity of the financial services industry, which includes small and regional banks and credit unions as well as large banks. These comments also show that community and local institutions face the same threats of fraud and identity theft, and need the same tools for preventing and controlling those threats, as the nation's largest financial institutions.

information to complete transactions continues to be effective and secure.” Visa Comments at 1.

¹⁴ IBAT Comments at 1.

¹⁵ California and Nevada Credit Union Comments at 1.

¹⁶ SAFE Comments at 1.

¹⁷ ICUL Comments at 1.

¹⁸ CUNA Comments at 1.

II. COMMENTERS AGREE THAT THE PROPOSED RELIEF WILL REDUCE PRIVACY AND SECURITY RISKS

The Commission’s Public Notice of November 6, 2014 asks commenters specifically to address “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.”¹⁹ Commenters responding to this question overwhelmingly agreed that the relief requested in the *Petition* *would* reduce the privacy and security risks posed by fraud, data breaches and identity theft.

Notably, the American Financial Services Association states that “Informational messages sent to wireless numbers reduce privacy and security risks proactively so that fraud, data security breaches, and identity theft are less likely to occur in the first place.”²⁰ Similarly, the Online Trust Alliance comments that granting the *Petition* “will facilitate prompt and efficient communication of time-sensitive information that can both limit the occurrence and impact of online crime and identity theft.”²¹

Several comments describe specific ways in which prompt customer communications can make “fraud, data security breaches, and identity theft less likely to occur in the first place.” MasterCard, for example, points out that if a cardholder promptly confirms that a transaction was fraudulent, the card issuer not only can reverse the transaction, but can suggest steps — such as card reissuance — that will prevent

¹⁹ *Consumer and Governmental Affairs Bureau Seeks Comment on Petition for Exemption filed by the American Bankers Association*, CG Docket No. 02-278 (Public Notice Nov. 6, 2014) (“Notice”) at 2.

²⁰ AFSA Comments at 2.

²¹ OTA Comments at 2.

future fraudulent transactions on the same account.²² Similarly, the Future of Privacy Forum notes that by encouraging customers to take proactive steps such as placing fraud alerts on their credit reports or subscribing to credit monitoring services, remediation messages can prevent misuse of newly-issued credit cards by third parties.²³ The Credit Union National Association, responding specifically to the Commission’s question, states that customers who receive prompt notification of data security breaches “can immediately initiate remedial action, such as aggressive account monitoring to locate fraudulent activity, credit report monitoring, or filing a freeze on applications for new credit.”²⁴ These excerpts are merely a few examples of the commenters’ consensus position that the relief requested would encourage prompt, proactive responses that would prevent, and significantly reduce the impact of, fraud and identity theft.²⁵

Two commenters point out that the requested relief also would help to prevent fraud targeted directly against customer accounts at financial institutions:

Fraud alerts also play an important role when it comes to fraud that is perpetrated on the consumer’s bank account itself, such as ACH fraud, wire fraud, person-to-person transfer fraud, and bill pay fraud. In each of these cases, immediate notification of the potential fraud can mean the difference between being able to recover the stolen funds and having the funds be transferred overseas and out of reach forever. It is crucial that a financial institution be able to deliver a fraud alert to the affected consumer within hours, and not days, of the potentially fraudulent transaction in order to recover the stolen funds and prevent future fraudulent transactions.²⁶

²² MasterCard Comments at 6-7.

²³ OTA Comments at 2; FPF Comments at 8.

²⁴ CUNA Comments at 3-4.

²⁵ *See also* California and Nevada Credit Union League Comments at 2; FirstBank Comments at 2; SAFE Comments at 1; PSCU Comments at 1; FSR Comments at 2; Visa Comments at 2; ITC Comments at 1; ICUL Comments at 1; OTA Comments at 2.

²⁶ IBAT Comments at 2; *see also* IBC Comments at 5.

Finally, no commenter — not even the two individuals who opposed the Petition — has plausibly denied that the requested relief will reduce fraud and identity theft. Joe Shields and Gerald Roylance both assert that financial institutions and merchants should reduce fraud and identity theft by improving their fraud prevention practices rather than communicating more efficiently with customers; but neither commenter recognizes that prompt customer alerts and notifications are more than good customer treatment strategies; they are themselves prevention practices that avoid incidents of possible fraud from proliferating.²⁷

Financial institutions dedicate hundreds of millions of dollars annually to data security and adhere to strict regulatory and network requirements. Regrettably, threats to data security continue to grow and are ever-changing. Under the circumstances, empowering consumers to take action to protect themselves is an essential component of any fraud prevention program. Until we can be sure that no unauthorized transaction will ever be attempted and no customer information will ever be breached, the need to notify customers promptly and efficiently of those events, and to advise them of appropriate remedial and preventive actions, will remain.

III. THE COMMENTS CONFIRM THAT THE LITIGATION THREAT INHIBITS CRITICAL CONSUMER COMMUNICATIONS

The comments confirm that institutions are inhibited from sending automated, time-critical communications to their customers because of the ever-increasing threat of litigation. Commenters expressing this concern are not just the large institutions that have

²⁷ Comments of Joe Shields on the American Bankers Association Petition for Exemption, CG Docket No. 02-278 (filed Dec. 8, 2014) (“Shields Comments”) at 5; Gerald Roylance’s Comments re American Bankers Association Petition, CG Docket No. 02-278 (filed Dec. 8, 2014) (“Roylance Comments”) at 3.

been targets of the plaintiffs' bar so far; they include independent community banks and credit unions, which are especially vulnerable to litigation costs and the uncapped damages routinely awarded to class action attorneys. For example, the Independent Bankers Association of Texas states that "IBAT's members will continue to be faced with the threat of potential TCPA consumer class action" if they send messages of the kind described in the Petition.²⁸ Similarly, the Credit Union National Association states that "[l]itigation alleging that automated calls were placed to mobile devices without prior express consent makes financial institutions leery of reaching consumers' mobile devices by automated means."²⁹

The comments also make clear that financial institutions cannot avoid liability simply by sending fraud alerts and other time-critical calls only to customer-provided mobile contact numbers, in reliance upon this Commission's determination that providing such a number to a business constitutes consent to be called by the business at that number.³⁰ As International Bancshares Corporation points out, the courts have not universally accepted the Commission's interpretation of the prior express consent requirement, and the Commission's recent statements to the effect that the scope of each consent must be determined by its context has given plaintiffs' lawyers even more encouragement to challenge all consents as inadequate.³¹ Also, as other commenters observe, plaintiffs'

²⁸ IBAT Comments at 1.

²⁹ CUNA Comments at 4.

³⁰ *Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991*, 7 FCC Rcd 8752, 8769 (1992) ("1992 Order").

³¹ IBS Comments at 2-3; *see also* letter from Jonathan B. Sallet, General Counsel, Federal Communications Commission, to Catherine O. Wolfe, Clerk, United States Court of Appeals for the Second Circuit, in Case No. 13-1362 (June 30, 2014); *GroupMe, Inc./Skype Communications S.A.R.L. Petition for Expedited Declaratory Ruling*, 29 FCC Rcd 3442 (2014); *Mais v. Gulf Coast Collection Bureau, Inc.*, Case No. 11-61936-CIV,

lawyers continue to challenge calls placed to consumer-provided numbers that have been reassigned without the knowledge of the callers.³² In the face of these realities, legal risk will continue to discourage financial institutions from communicating with their customers using the most efficient means, unless the relief requested in the Petition is granted.

IV. THE COMMENTS DO NOT SUPPORT THE IMPOSITION OF ADDITIONAL CONDITIONS

The Commission’s Public Notice asks whether the Commission “should consider additional or modified conditions to protect consumers from unwanted communications and from fraud, identity theft and data security breaches?”³³

The comments respond to this question with overwhelming support for the conditions proposed in the Petition. Only two commenters propose an additional condition — a requirement that recipients of the four categories of informational communications described in the Petition have a right and mechanism for opting out of future such messages.³⁴

The Petition suggested that an opt-out requirement be imposed for money transfer notifications, but not for messages concerning possible fraud, data security breach or remediation. As the Petition points out, fraud alerts, data security breach notifications and remediation messages are sent for the consumer’s benefit and, in the case of breach

2013 WL 1899616 (S.D. Fla. 2013); *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); *Kolinek v. Walgreen Co.*, 2014 U.S. Dist. LEXIS 15986, 2014 WL 518174 (N.D. Ill. Feb. 20, 2014), *vacated*, 2014 U.S. Dist. LEXIS 91554 (N.D. Ill. July 7, 2014).

³² *See, e.g.,* *Osorio v. State Farm Bank*, No. 13-10951, DC Docket NO. 0:11-cv-61880-DMM (11th Cir. 2014); *Soppet v. Enhanced Recovery Co.*, 679 F.3d 637 (7th Cir. 2012).

³³ Public Notice at 2.

³⁴ Roylance Comments; Noble Systems Comments.

notifications, are required by law. A customer's decision to opt out of receiving such messages will have only negative consequences that he or she may not have considered (or may have discounted) at the time. In the case of a fraud alert, there may be pending a denial of a transaction that the customer has authorized, but has nevertheless triggered fraud screens. Customers likely would not be considering the value of being consulted in a timely manner about such authorized, but suspended, transactions when opting out of an alert program. In the case of a breach notification or remediation message, a customer's decision to opt-out will result in transmission of the same message via channels that are less efficient and less likely to permit timely remedial action. Given that the proposed messages will be sent on a free-to-end-user basis, will not contain marketing content, and will be limited in scope and duration according to the conditions proposed in the Petition, there is no need to impose an opt-out requirement on those messages.

In fact, creating an opt-out right for the messages described in the Petition would harm, rather than advance, customer privacy, by exchanging a negligible privacy benefit for an increased risk that consumers will suffer the severe privacy harms of stolen information, fraud and identity theft.

Finally, as the Independent Bankers Association of Texas points out, "the cost of managing an opt-out process would be significant for community banks and would greatly outweigh any possible benefits."³⁵

³⁵ IBAT Comments at 3.

CONCLUSION

The comments in this proceeding show overwhelming support for ABA's Petition from a variety of industries, from smaller as well as larger companies, and from organizations dedicated to the protection of consumer privacy and data security. The record in this proceeding firmly supports a conclusion that the relief requested will substantially advance the privacy of customer information and security from fraud and identity theft, while also protecting the interests the TCPA is intended to protect. Accordingly, ABA requests that its Petition be promptly granted.

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

December 19, 2014