The Kennedy Privacy Law Firm

1050 30th Street, NW
Washington, DC 20007
www.kennedyonprivacy.com

Charles H. Kennedy
(202) 250-3704
(202) 450-0708
ckennedy@kennedyonprivacy.com

May 22, 2015

Via ECFS

Ms. Marlene H. Dortch
Secretary
Federal Communications Commission
445 12th Street, N.W.
Washington, DC 20554

Re: *Ex Parte* Filing, CG Docket No. 02-278

Dear Ms. Dortch:

The *ex parte* letter filed with this Commission on April 28, 2015 by the National Consumer Law Center (NCLC) and the National Association of Consumer Advocates (NACA) shows that the differences between those organizations and the American Bankers Association (ABA), concerning ABA's petition for exemption under section 227(b)(2)(C) of the Communications Act, have largely been resolved, leaving no substantive obstacles to the prompt granting of the ABA Petition.[1]

[1] Letter from Margot Saunders, Counsel, National Consumer Law Center to Marlene Dortch, Secretary, Federal Communications Commission in CG Docket No. 02-278 (Apr. 28, 2015) (NCLC Letter); Petition for Exemption of the American Bankers Association, CG Docket No. 02-278) (filed Oct. 14, 2014) (ABA Petition). The NCLC Letter was filed on behalf of that organization and the National Association of Consumer Advocates.

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.

The differences between the organizations' positions already were substantially narrowed when ABA, in an *ex parte* letter filed on February 5, 2015, agreed to give consumers an opportunity to opt out of receiving further texts in each message category identified in the ABA Petition.[2] Now, in their letter of April 28, 2015, NCLC and NACA concede that automated fraud alert and money transfer messages are appropriate and in the consumers' interests, and ask only that those messages be subject to additional conditions intended to protect the privacy of consumers and avoid inconvenience to unintended recipients.[3] NCLC/NACA also maintain that data security breaches, alone of the categories identified in the ABA Petition, lack sufficient urgency to justify automated voice or text notifications to affected consumers.[4]

As ABA explains below, NCLC/NACA's remaining concerns, which are hardly

---

[2] Letter from Charles H. Kennedy, Counsel for American Bankers Association, to Marlene Dortch, Secretary, Federal Communications Commission, CG Docket No. 02-278 (Feb. 5, 2015). Conditioning of the proposed exemption on the provision of an opt-out opportunity was the most consistent demand of commenters opposing the ABA Petition. *See* Letter from Margot Saunders, Counsel, National Consumer Law Center to Marlene Dortch, Secretary, Federal Communications Commission, in CG Docket No. 02-278 (Dec. 19, 2014) (representing NCLC, ACA and other organizations); Comments of Noble Systems Corporation in CG Docket No. 02-278 (Dec. 8, 2014); Gerald Roylance's Comments re American Bankers Association Petition in CG Docket No. 02-278 (Dec. 8, 2014).

[3] NCLC Letter at 3-6. NCLC/ACA concede that a "fraud alert that triggers the suspension of an account, either a bank account or a credit card action, is something that most consumers will want to know about immediately;" and that "[c]alls regarding wire transfers are appropriate for [the requested] exemption." *Id.* at 4-5.

[4] *Id.* at 4. The ABA Petition requests exemption under section 227(b)(2)(C) for automated voice and text messages to customers 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. ABA Petition at 3.

unique to automated calls and texts, do not support additional limitations on the relief ABA has requested. ABA members already are subject to substantial privacy and data security regulations, and already take measures intended to protect the privacy of consumers and avoid inconvenience to unintended recipients. Also, contrary to NCLC/NACA's claims, data security breaches are an increasing consumer threat that can best be contained if consumers react promptly to protect their identities and private financial information. The Commission can contribute significantly to the containment of data breaches by approving the use of automated texts and voice communications to give timely notice of those events.

The paucity of NCLC/NACA's remaining objections confirms that granting the ABA Petition now is the right thing to do.[5]

I. NCLC/NACA'S CONCERNS DO NOT SUPPORT THE IMPOSITION OF ADDITIONAL CONDITIONS

NCLC/NACA express concern that if a financial institution's non-telemarketing message inadvertently is delivered to an unintended recipient, the intended recipient might suffer a loss of privacy, and the actual recipient might be inconvenienced. Accordingly, NCLC/NACA ask the Commission to impose the following conditions on the proposed exemption: (1) information provided by free-to-end-user calls and texts must not be of such a personal nature that it would violate the privacy of the intended called party for another person to receive the calls; (2) the information in the calls and texts must be targeted to the

[5] The NCLC Letter discusses a number of pending requests for relief, including those that ask the Commission to resolve the problem of calls inadvertently placed to reassigned numbers and those that concern calls from healthcare organizations. ABA responds here only to those arguments that appear to be directed at its Petition for Exemption filed with the Commission on October 14, 2014.

intended recipient such that the called party does not embark on a course of action that is not relevant to her; (3) the calls and texts must be permitted only when the caller has a reasonable basis to believe that the called party is the intended party; and (4) the number of calls must be limited.[6]

All communication channels used to communicate with customers about their accounts, including postal mail, email and manual telephone calls, present the same issues of privacy and convenience identified in the NCLC Letter. The informational messages described in the ABA Petition do not present different or greater risks, and do not call for the imposition of special conditions not applicable to other media. Moreover, the messaging programs described in the ABA Petition already satisfy the privacy and convenience concerns raised in the NCLC letter and need not be subjected to conditions beyond those ABA has proposed.

A. The Proposed Texts will not Contain Consumers' Personal Information

Contrary to NCLC/NACA's concerns, the information contained in fraud alert, breach notification, remediation and money transfer messages cannot be exploited by unintended recipients to commit identity theft or compromise customer privacy.

ABA members are subject to extensive privacy and data security regulations and standards that require financial institutions to safeguard the security of all customer personal information, in any medium in which that information is stored and when transmitted by any communication channel.

For example, the Safeguards Rule adopted pursuant to the Gramm-Leach-Bliley Act

[6] NCLC Letter at 4-6.

requires financial institutions to safeguard the security, confidentiality, and integrity of all nonpublic personal information, including all personally identifiable information maintained by the financial institution that is not publicly available.[7] Financial institutions would violate the Safeguards Rule if they transmitted "credit card information or other sensitive financial data" over an insecure channel.[8]

Similarly, the Payment Card Industry Data Security Standard (PCI-DSS) requires any entity that stores, processes or transmits payment card data to avoid sending such data over open, public networks or to do so only when the transmission is protected by strong encryption.[9]

Accordingly, in compliance with applicable requirements and as part of our members' ongoing efforts to protect customers' privacy, calls and texts that ask a customer to confirm a suspicious transaction do not include the customer's complete account number or any other nonpublic financial information. For example, a typical text request to verify a suspicious charge might consist of the following:

> ABC Bank fraud alert: Did you just attempt a $1218.13 charge on Card ending in XXXX at [merchant name]? Reply 1 if yes, 2 to speak to an agent. STOP to opt out.[10]

---

[7] Standards for Safeguarding Customer Information, 16 C.F.R. Part 314.1, adopted pursuant to Gramm-Leach-Bliley Financial Modernization Act, Pub. L. No. 106-102, 113 Stat. 1338 (1999), codified at various sections of 12 United States Code and 15 United States Code.

[8] *See* Federal Trade Commission, "Financial Institutions and Customer Information: Complying with the Safeguards Rule," available at https://www.ftc.gov/tips-advice/business-center/guidance/financial-institutions-customer-information-complying.

[9] Payment Card Industry (PCI) Data Security Standard, Requirements and Security Assessment Procedures, vers. 2.0 (October 2010), Requirement 4.1, available at https://www.pcisecuritystandards.org/security_standards/.

[10] The following are additional examples of messages that are being sent, or would be sent if the proposed exemption were granted, by ABA members to verify a suspicious purchase,

That sample message contains no information that could be used to commit identity theft against the intended recipient. Similarly, the proposed data security breach notifications and remediation messages will not contain account numbers, access codes or other information concerning the affected accounts that could be used by unintended recipients or hackers to commit identity theft. Messages providing notice of a money transfer will provide a link or telephone number that the recipient can use to arrange for receipt of transferred funds, but will not furnish account numbers of the transferee or transferor or other sensitive information. Accordingly, if one of the messages described in the ABA Petition inadvertently is delivered to the wrong party, because a customer contact number has been reassigned without the bank's knowledge or for any other reason, the

---

website login, address change, replacement card request or other action taken regarding an account. None of these messages contains information that could be used to commit identity theft against the intended recipient:

For verification of a suspicious bank website login: "ABC Bank Re-authentication Key: 875984 Enter online at prompt."

For verification of an address change: "ABC Bank Fraud Alert: Address change completed on Card ending 12000. If not requested, call the number on back of card."; and "ABC Bank Fraud Alert: Did you just initiate an address change on Card ending 12000? Reply 1 if yes, 2 to speak to an agent."

For verification of a request for a replacement card: "ABC Bank Fraud Alert: Replacement card requested on Card ending 12000. If not requested, call the number on back of card."; and "ABC Bank Fraud Alert: Did you just request a replacement of card ending 12000? Reply 1 if yes, 2 to speak to an agent."

For verification of receipt of card: "ABC Bank Fraud Alert: Did you receive your recent issuance of Card ending 12000? If yes, reply 1 to activate, or reply 2 to speak to an agent if Card not received."

For security on select online purchases: "875984 is your One Time Password for your online purchase on ABC Bank card ending 12000. If not requested, call the number on back of card."

customer's privacy or data security will not be compromised.

Given the extensive privacy and security requirements to which financial institutions are subject as well as the compliant practices already in place, there is no need for the Commission to address NCLC/NACA's privacy concerns by adding additional conditions to its order granting ABA's requested exemption. In fact, the vaguely-worded conditions suggested by NCLC/NACA, using undefined terms such as "privacy" and "personal nature," would add nothing to existing data security regulations and standards except confusion and an invitation to needless litigation.

B. The Proposed Texts will not Encourage Unnecessary Action by Unintended Recipients

NCLC/NACA also are concerned that when a fraud alert, data breach notification or other message is inadvertently sent to a person other than the intended recipient, the recipient may waste time and effort responding to the message. In order to minimize this potential inconvenience, NCLC/NACA urge the Commission to condition the requested exemption on ABA members' commitment to target the subject messages to intended recipients.

The requested condition is unnecessary. ABA members' fraud alerts and other informational messages will include sufficient information, such as the name of the sending financial institution and the type of payment card involved, to permit recipients to determine if the messages are intended for them. Requiring additional, personally identifiable information in automated texts and calls would add little to customer convenience, would be difficult to accomplish within the constraints of the text messaging format, and significantly, would undermine the privacy and data security interests that

NCLC/NACA claim to support.[11]

C. The Proposed Messages will be sent only to Persons who are Reasonably Believed to be the Intended Recipients

There also is no need for a condition requiring ABA members to have a "reasonable basis to believe that the called party is the intended party," with the burden of proving such reasonableness falling on the caller. The phrase "reasonable basis" introduces a vague standard that is likely to be exploited for litigation purposes but will add nothing to the incentives ABA members already have to ensure that messages reach their intended recipients. Messages sent pursuant to the requested exemption will be transmitted on a free-to-end-user basis, making misdirected messages a cost to the sender rather than the recipient. Moreover, the absence of marketing content in the proposed messages means that a misdirected message will not have even the incidental benefit of promoting the sender's product or service. Accordingly, ABA members currently have ample incentives to take reasonable measures to ensure that their informational messages are reaching the intended recipients, and the condition proposed by NCLC/NACA will add nothing to those incentives.

As the ABA Petition already proposes, "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," and "[i]n the case of money transfer notices, messages will be sent

[11] In addition, all of the informational messages ABA members propose to send include a means for customers to respond to the sending financial institution, giving recipients a convenient means to confirm that they are intended recipients.

only to the designated recipients of transferred funds."[12] Also, use of automated rather than manual dialing technology, which will be facilitated when the Commission grants ABA's Petition, substantially reduces the incidence of erroneous dialing.

As petitions and filings pending before the Commission note, even the best compliance measures cannot prevent entirely 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 or a letter or email message is read by another household member. However, this risk is not unique to automated calling and texting, and denying or adding unnecessary conditions to the ABA Petition will not reduce those risks.

D. ABA Already Accepts Reasonable Limits on the Number of Messages Subject to the Exemption

The NCLC Letter asks the Commission to limit the number of messages that may be sent pursuant to the exemption, suggesting that "one call or text, or possibly one original call, and an additional reminder, is quite sufficient."[13]

In fact, the ABA Petition already proposes a set of conditions, tailored to consumers' needs and the limited purpose of each informational communication, that will protect consumers from receiving excessive numbers of messages.

Specifically, ABA has proposed that the exemption for breach and fraud-related communications should permit three such messages to be sent each day for a maximum of three days, if the customer does not respond.[14] This proposal reflects the need for customers

[12] ABA Petition at 17.

[13] NCLC Letter at 5.

[14] ABA Petition at 19.

to be given an adequate opportunity to receive these important messages, but also acknowledges that the need to take prompt corrective action limits the time during which attempts to reach the customer would be beneficial and should continue.

Similarly, ABA has requested 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.[15] Consumers' interests would not be served if, for example, a financial institution could not advise a customer who has been the victim of fraud of the remediation steps to be taken by the bank and the customer.

ABA already has agreed to send only one automated, free-to-end-user notice of a mobile money transfer.[16]

Finally, consumers will have the ultimate means of preventing the receipt of excessive numbers of informational messages: *i.e.*, the opt-out opportunity that will accompany each message in all four of the categories proposed in the ABA Petition.

NCLC/NACA have not explained why the limits on numbers of messages already proposed by ABA are insufficient, and there is therefore no need to impose any additional or different conditions.

II. DATA SECURITY BREACH NOTIFICATIONS REQUIRE PROMPT, AUTOMATED NOTIFICATIONS TO AFFECTED INDIVIDUALS

Although NCLC/NACA effectively concede that the requested exemption is

[15] *Id.*

[16] *Id.* at 20.

appropriate as to most of the communication categories described in the ABA Petition, they oppose grant of the exemption for messages that notify affected consumers of breaches in the security of their personal information. According to the NCLC Letter, "[a]fter a data breach there is little a consumer can do about it, other than keep an eye on her accounts and her credit."[17] Thus, they assert, a "letter [notice] generally suffices."[18]

NCLC/NACA severely understate the urgency of data security breach incidents and the ability of consumers to take action to prevent consequent identity theft. [19] As commenters in this proceeding have pointed out, 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."[20] Similarly, the Federal Trade

---

[17] NCLC Letter at 4.

[18] *Id.*

[19] ABA also rejects NCLC/NACA's claim that the availability of the "emergency exception" to the prior express consent requirement makes the ABA Petition unnecessary. As ABA previously has pointed out, although ABA believes that the emergency exception is and should be a sufficient ground on which to base the sending of fraud and identity theft related messages, the courts and the FCC have not clarified the scope of that exception as applied to situations that do not present a risk of death, injury or harm to public safety. *See* letter from Charles H. Kennedy, counsel for American Bankers Association, to Marlene Dortch, Secretary, Federal Communications Commission, CG Docket No. 02-278 (Jan. 26, 2015). In the present litigation environment, financial institutions simply cannot assume that reliance on the emergency exception will succeed when challenged.

[20] Comments of the Credit Union National Association in Support of Petition for Exemption of American Bankers Association, CG Docket No. 02-278 (Dec. 8, 2014) at 3-4; *see also* Future of Privacy Forum Comments, CG Docket No. 02-278 (Dec. 8, 2014) at 10; Identity Theft Council Comments, CG Docket No. 02-278 (Dec. 8, 2014) at 8.

Commission urges consumers who receive data security breach notifications to take various actions, including placing a fraud alert and obtaining a credit report "right away."[21] Organizations such as the Privacy Rights Clearinghouse offer similar advice.[22]

NCLC/NACA also fail to acknowledge the rapid proliferation of fraud and identity theft. Data breach incidents affecting bank customers have increased 27.5% since 2013, and a Javelin Strategy & Research study shows that an increasing percentage of persons affected by such breaches are victims of identity theft (up from 1 person in 9 in 2010 to 1 person in 3 in 2014).

Both unauthorized transactions and identity theft impose substantial costs on consumers. Although banks reimburse customers for the vast majority of their direct loss, out-of-pocket expenses for identity theft victims range from an average of $63 for misuse of a credit card to $289 for fraud involving a stolen Social Security number — numbers that do not include the consumer's lost time and stress. Customers also report that declined payment card transactions, many of which could be prevented by prompt communication with customers at their mobile devices, cause embarrassment and inconvenience. In fact, one ABA member reports that 60% of its consumer complaints concerning questionable transactions refer to the embarrassment of having a transaction declined at the point of sale. The general experience of ABA members is that consumers expect their banks to contact them

[21] Federal Trade Commission, "What to do Right Away," available at https://www.identitytheft.gov/#what-to-do-right-away.

[22] Privacy Rights Clearinghouse, "How to Deal with a Security Breach," available at https://www.privacyrights.org/how-to-deal-security-breach#FigureOutWhat.

promptly to resolve issues that might result in declined transactions, fraudulent transactions or identity theft, and to convey information needed to restore their accounts and minimize loss and inconvenience.

Addressing data breaches quickly also reduces their profitability to the hacker and reduces the incentive to commit a data breach in the first place. Prompt notification of consumers of a data breach is thus an important part of the larger effort by Congress, the Administration, state officials and affected industries to combat cyber security threats. Granting the ABA Petition could be one of this Commission's most substantial contributions to that effort.

CONCLUSION

The NCLC Letter shows that the differences between ABA and NCLC/NACA have narrowed to a few objections that largely are anticipated and resolved by the ABA Petition and the conditions ABA already has agreed to accept. Accordingly, there are no substantive obstacles to the prompt granting of the ABA Petition, and the Commission should move promptly to approve a limited exemption that plainly will serve the public interest.

Respectfully submitted,

/s/ Charles H. Kennedy

Charles H. Kennedy