



**International Bancshares  
Corporation**

---

December 8, 2014

***Via Electronic Comment Filing System: <http://apps.fcc.gov/ecfs/>***

Ms. Christina Clearwater  
Consumer and Governmental Affairs Bureau  
Federal Communications Commission  
445 12th Street, SW  
Washington, DC 20554

Re: CG Docket No. 02-278; Comments to Petition for Exemption ("Petition") of the American Bankers Association ("ABA") Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991 ("TCPA")

Dear Ms. Clearwater:

The following comments are submitted on behalf of International Bancshares Corporation ("IBC"), a multi-bank financial holding company headquartered in Laredo, Texas. IBC holds four state nonmember banks serving Texas and Oklahoma. With over \$12 billion in total consolidated assets, IBC is the largest Hispanic-owned financial holding company in the continental United States. IBC is a publicly-traded holding company. We appreciate the opportunity to comment on the ABA's Petition.

IBC's business model includes an array of retail products for its consumer customers. It is currently in the process of enhancing its online banking program to include a more robust mobile banking platform. Existing customers as well as new customers will be able to use this new program when it is launched. Thus, it is particularly important to us that the very rigid requirements relating to express prior consent be relaxed as to the requests discussed below.

I. Overview of the Petition

On October 14, 2014, the ABA filed the above-mentioned Petition with the Federal Communications Commission ("FCC"), requesting an exemption from the requirement under the TCPA that an entity obtain prior express consent from a consumer before sending four categories of messages: 1) transactions and events that suggest a risk of fraud or identity theft; 2) possible breaches of consumers' 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. In its Petition, the ABA highlights the need for the exemption in order to alleviate concerns for financial institutions that sending such messages may subject the financial institution to TCPA consumer class action lawsuits. If granted, the proposed exemption would enable financial institutions to fulfill legal requirements and protect consumers by sending these types of messages without prior express consent from the message recipients.

5702899.2  
5702899.2

The ABA proposes in its Petition that such messages be exempt only when they are sent without charge to the recipient and meet the following six conditions:

- 1) Automated messages subject to the exemption will be sent only to the telephone numbers of consumers to whom the alert is directed;
- 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 message;
- 5) Financial institutions will send no more automated messages than are required to complete the communications' intended purpose; and
- 6) Recipients of money transfer notifications will have the opportunity to opt out of future such communications.

## II. Comments to Petition

IBC strongly supports the ABA's Petition requesting that the FCC exempt four categories of messages sent by financial institutions from the requirement under the TCPA that autodialed messages, text messages, and prerecorded messages placed on landline phones be sent with prior express consent. The exemption would reduce burdens on financial institutions and provide additional protections to consumers.

As the TCPA and its implementing regulation, 12 C.F.R. § 64.1200, currently exist, there is confusion as to what constitutes the "prior express consent" required to send text messages, call consumers' mobile phones using an autodialer, and place pre-recorded messages to landline phones. IBC agrees with the FCC's ruling that the "prior express consent" standard may be satisfied by consumers providing their phone number to the intended caller.<sup>1</sup> Courts have not universally accepted the FCC's ruling on this though.<sup>2</sup>

---

<sup>1</sup> 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).

<sup>2</sup> 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*, 2008 WL 5000528 (N.D. Cal. 2008).

In one case, the plaintiff consumer provided the consumer's mobile phone number to a Walgreen pharmacy at the time of prescription pick up. Walgreen sent pre-recorded messages to her mobile phone with refill reminders. The consumer sued and Walgreen filed a motion dismiss based on the FCC's ruling. The Court denied Walgreen's motion to dismiss, as questions remained about the context under which the consumer provided her phone number and the consumer's expectation of how the number would be used.<sup>3</sup>

IBC is supportive of the ABA's exemption requested in its Petition because, without the exemption, IBC will continue to be faced with the threat of potential TCPA consumer class action lawsuits should it choose to send such messages without prior express consent. Not sending these messages hinders IBC from fulfilling legal requirements and acting to protect consumers from fraud, identity theft, and data breaches. In our experience, our customers provide us with their mobile numbers with the full expectation that they will be used appropriately to communicate with them.

#### A. Reduce Burdens on Financial Institutions

Enabling financial institutions to send these four types of messages will allow financial institutions to decrease costs while also making such messages more effective and accelerating delivery of those messages. Currently, financial institutions must hand-dial affected consumers in order to deliver such messages and not subject themselves to potential liability under the TCPA. Hand-dialing takes significantly more time and has a higher error rate (i.e., mis-keying telephone numbers and reaching unintended recipients). The ABA's Petition notes that emails are opened less frequently than text messages.<sup>4</sup> By automating these messages, through autodialed calls and/or text messages, financial institutions can significantly save on the costs, through decreased staffing, to deliver these messages while also providing added consumer protections. (See Section II(B), below).

The exemption would also decrease fraud-related losses for financial institutions. In 2009, 62 percent of reported debit card fraud losses were incurred by banks, while only 38 percent of losses were incurred by merchants.<sup>5</sup> By making fraud and identity theft alerts, data breach notifications, and remediation messages more effective and delivering them more quickly, financial institutions are able to prevent customers from falling victim to future fraudulent transactions. This in turn reduces losses for financial institutions, who usually incur the liability from fraudulent transactions, under both Regulation E and "zero liability" provisions of the card networks.

---

<sup>3</sup> *Kolinek v. Walgreen Co.*, 2014 U.S. Dist. LEXIS 15986, 2014 WL 518174 (N.D. Ill. Feb. 10, 2014), vacated, 2014 U.S. Dist. LEXIS 91554 (N.D. Ill. July 7, 2014).

<sup>4</sup> "In contrast to the 98% success rate of text messaging, only 22% of email messages are opened."

<sup>5</sup> *Protecting Consumer Information: Can Data Breaches be Prevented?*, 113<sup>th</sup> Cong. (Feb. 5, 2014) (Statement for the Record on behalf of the American Bankers Association before the Committee on Energy and Commerce).

Currently, IBC does not have full functionality for fraud alerts via text messaging. And without the approval of this Petition, the possibility of acquiring an effective program with reasonable start up and ongoing costs is severely impaired. Innovation is set back without rational accommodation of changes in consumer expectations, technology changes, and bank needs.

**B. Provide Increased Consumer Protections**

IBC strives to provide the highest level of consumer protection possible, but IBC's ability to provide additional consumer protections is currently limited by the threat of lawsuits brought under the TCPA for messages that are sent without consumers' prior express consent. Financial institutions like IBC are increasingly being targeted by record-breaking class action settlements like the recent \$75 million settlement involving Capital One. The threat of these settlements has prevented IBC from utilizing more efficient and effective means of sending fraud and identity theft alerts, data breach notifications, and data breach remediation messages to IBC's customers.

Alerting its customers to potential fraud and identity theft is very important to IBC, whose motto is "We do more". As the ABA noted in its Petition, identity theft, fraud, and data security breaches have reached historically high levels. IBC has sophisticated methods of detecting fraud, but IBC's monitoring is only as effective as the method of delivery for its fraud alerts. IBC does not send a fraud alert for each and every red flag that may make a transaction suspicious. Rather, IBC uses a refined algorithm to analyze various pieces of data and identify the red flags that are most likely to be suspicious. IBC then issues fraud and identity theft alerts for the transactions that are determined to have a high probability of fraud. Due to the high likelihood that such transactions are fraudulent, it is crucial that these fraud alerts be delivered in an effective and efficient method.

Effective fraud prevention requires the earliest possible contact with the affected consumer. IBC wants to notify its customers in the most efficient and effective means possible, not only to comply with the various federal and state statutes requiring financial institutions to notify affected customers, but also to protect the customers themselves. IBC agrees with the ABA that automated communications are best suited to successfully notify customers of fraud, identity theft, and data security breaches in the most efficient and effective way possible. A significant number of IBC's customers have mobile phone numbers and numerous customers maintain only a mobile phone number and not a landline phone number. Any impediment to automating these notifications penalizes consumers. It often becomes impractical, if not impossible, for financial institutions to notify each and every affected customer within prescribed timeframes and in time for the consumer to take action on the notification to prevent future harm if automated means are not available. When large numbers of affected consumers are involved, financial institutions simply cannot hand dial that many customers' phone numbers within the requisite time periods. Customers not called may not learn about potential fraud, identity theft, or data security breaches until after additional fraud has already occurred, in which case the financial institution will likely incur the liability. Even if the financial institution incurs liability, however, the consumer will still be faced with requesting new debit or credit cards, updating cardholder information for auto-billed transactions, filing unauthorized transaction claims with financial institutions, and putting identity theft alerts on the consumer's account.

Fraud alerts are important for transactions that occur across a wide variety of different channels and are not limited to fraud that occurs when a consumer's debit or credit card number is stolen from a retailer. 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.

Data breach notifications can also be a major communication issue for financial institutions. As discussed earlier, financial institutions currently alert affected consumers of data breaches and provide remediation messages by hand-dialing or emailing such consumers. Because this process takes significantly more time and financial institutions are less successful in reaching consumers, some financial institutions are unable to successfully reach consumers within the periods prescribed by state statutes and within a reasonable period of time for consumers to take the actions recommended in the remediation messages. If these messages were able to be sent through autodialed calls and/or text messages, more consumers would be successfully reached. Autodialed calls could be made more quickly, thus reaching more consumers in a quicker period of time. Text messages could be sent immediately and all at one time. Moreover, text messages have a higher rate of success in being read by consumers than telephone calls have in being answered or voicemails have in being listened to. Thus, text messages would be more effective, prevent additional fraud and identity theft, and decrease losses to financial institutions.

It is also important to point out that data breach notifications and remediation messages are sent by financial institutions not only for breaches that occur at the financial institutions themselves, but also for breaches at merchants where the financial institutions' customers have shopped. While it may be less likely for a consumer's financial institution to suffer a breach, it is far less uncommon for a merchant where the consumer has shopped to suffer a breach.<sup>6</sup> For this reason, the requested exemption would improve the effectiveness and speed at which financial institutions can notify consumers of data breaches, not only at financial institutions but also at any business where a consumer has conducted a financial transaction. If consumers do not quickly act to deal with at risk cards, there is a higher likelihood that fraudsters will use the compromised cards to make unauthorized transactions. While Regulation E provides a mechanism for the complaint process to proceed, the longer the delay in using this process, the more likely there will be further fraudulent transactions. This increases the cost to the innocent bank which issued the card and causes administrative stress for the customer.

---

<sup>6</sup> Financial institutions accounted for less than 8 percent of reported breaches from 2005 to 2013. *Protecting Consumer Information: Can Data Breaches be Prevented?*, 113<sup>th</sup> Cong. (Feb. 5, 2014) (Statement for the Record on behalf of the American Bankers Association before the Committee on Energy and Commerce).

The requested exemption would allow financial institutions to stay ahead of the technology curve by doing what consumers already do. Consumers increasingly use text messaging as a primary form of communication. As the ABA's Petition points out, more than 1 in 3 consumers prefer to receive fraud alerts through text messaging. By communication through consumers' preferred method of communication, financial institutions are more likely to get through to consumers.

The requested exemption would not pose any harm to consumers. Financial institutions have no incentive to send any more messages than are reasonably necessary to alert affected consumers of fraud, identity theft, and data security breaches. Such messages would not be exempt, creating liability for the institution. Further, excessive messages create "noise" and decrease the likelihood that legitimate alerts are ignored. Also, if the exemption is approved, the messages would be sent without any cost to the recipient and would not contain any solicitation, telemarketing, or advertising content; the messages would be purely transactional and for consumers' own protection.

While we understand that the goal behind the TCPA is to protect consumers, not permitting financial institutions to send these types of messages without prior express consent actually hinders this goal. Granting the exemption requested by the ABA will improve consumer protection by providing consumers with increased information about the tools available to protect themselves.

C. Reduced privacy and security risks

Approving the requested exemption would decrease privacy and security risks. Without providing financial institutions with an exemption to the rule that an entity must obtain prior express consent before autodialing or texting a consumer for the four types of messages identified in the Petition, some entities will continue to resort to hand-dialing consumers' telephone numbers for these types of messages. Hand-dialing results in a higher rate of calls placed to unintended recipients and increases the chances that personal information may inadvertently be disclosed to an individual other than the consumer to whom the information belongs. Thus, the exemption would decrease the privacy and security risks surrounding personal information.

As discussed earlier, more effective delivery of these messages will also increase the odds of consumers utilizing the tools available to them to prevent future privacy threats, such as requesting that an identity theft alert be placed on a consumer's account and requesting that an issuing financial institution replace a debit or credit card.

D. Number of messages

IBC supports the ABA's proposed condition regarding the number of messages that may be sent for fraud and identity theft alerts, data breach notifications, and remediation messages. IBC has no incentive to send an unnecessary number of these messages, but multiple messages are necessary in certain situations. As the ABA points out, the nature of these messages often requires them to be interactive such that the consumer can respond and the financial institution respond back. For this reason, IBC supports the proposed condition that such messages be limited to a maximum of three attempts per day for three days on each affected account and each affected co-borrower or co-cardholder.

E. Opt Outs

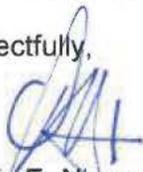
While the ABA does not propose a an opt-out mechanism for fraud and identity theft alerts, data breach notifications, and remediation messages as it does for money transfer messages, IBC would like to note that it strongly opposes any such opt-out mechanism for these three types of messages. These messages are extremely important in order to remedy existing fraud, identity theft, and data security issues and to prevent future such privacy and security issues. As mentioned above, the messages do not pose harm to consumers because they will be sent at no cost to the recipient, free of any solicitation, telemarketing, and advertising content, and be limited in number to the condition set forth in Section II(D), above.

F. Definition of Financial Institution

The ABA requests the proposed exemption for banks and other financial institutions. IBC requests that the FCC provide more clarity regarding which types of entities would be considered financial institutions under the requested exemption. Would a specific statutory definition of the term "financial institution" apply?

Thank you for your consideration.

Respectfully,



Dennis E. Nixon  
President