Before the
Federal Communications Commission
Washington, D.C. 20554

In the Matter of the	**)**	
	)	
Rules and Regulations Implementing	**)**	
	)	**CG Docket No. 02-278**
the Telephone Consumer Protection	**)**	
	)	
Act of 1991	**)**	

Reply Comments of Joe Shields on the Comments of the American Bankers Association on the American Bankers Association Petition for Exemption

I hereby submit these reply comments on the comments filed by the American Bankers Association (hereinafter "ABA") on the ABA Petition for Exemption. The commentor claims that the petition is overwhelmingly supported by commentors including consumer privacy organizations such as the Future of Privacy Forum (hereinafter "FOPF"). What ABA fails to admit is that most if not all commentors that support the petition will gain financially from the loss of consumer privacy if the ABA petition is granted. The FOPF is an organization that seeks self-regulation and best practices. History has shown that self-regulation never works. If self-regulation had worked the TCPA would not have been needed.

The FOPF repeats the banking industry's ad nauseam claim that the TCPA was: "…intended to restrict the use of aggressive telemarketing practices…" "The TCPA is not only directed at telephone solicitations, it is also directed at autodialer calls to cellular phones, as reflected by the different subsections of § 227, which create separate causes of action for telephone solicitations and automated calls to cellular phones." *Adamcik v. Credit Control Servs., Inc*., 832 F. Supp. 2d 744, 752 (W.D. Tex. 2011). See also: *In the Matter of Dialing Services LLC*, FCC 14-59, May 8th, 2014.

ABA's claim that breach notifications benefit consumers is false. ABA has not provided any evidence that breach notifications are proactive in nature. Most credit card fraud occurs within minutes of gaining access to a consumer's credit card information. Breach notifications are worthless in that context. Where consumer credit card information is taken from retail outlets it is most often used to create new accounts something that breach notifications are powerless to stop. The damage is done within minutes and breach notifications will only add to the misery of the victims.

I find this hyperbole about breach and identity theft messages amusing especially given the fact that the crime will already have happened. The only way to prevent breaches and identity theft is for the retail institutions and banks to secure their systems which they obviously haven't in the past. Most commentors supporting the ABA petition admit to the scope of the problem yet fail to admit the problem is of their own making.

The banking industry desire to punish consumers is misplaced – that will not solve the problem retailers have created by failing to secure their systems. The Point of Sale (hereinafter "POS") devices in use today transmit unencrypted data. Encrypting the transmission of consumer transactions through POS devices will reduce breach and identity theft tremendously – much more so than hundreds of millions of robocalls ever could.

As stated previously breach notifications are knee jerk reactions that come **after** a breach has occurred. Consequently, other than conforming to breach notification requirements they serve no other purpose. For example in the recent Staples breach where 1.1 million credit cards were compromised the breach occurred between July and September 2014. Yet Staples didn't acknowledge or even begin investigation of the

breach until October of 2014. Notifications of the result of the investigation are just now being sent to Staples customers. This lag between the actual breach and notification to the public occurs with every breach including the Target and Home Depot breaches. The only solutions that these breach notifications propose is an offer to pay for monitoring of consumer credit reports. There are ample channels to make such notifications such as email and mail which are far less intrusive, damaging and a threat to safety.

Mastercard chimed in on support for ABA's petition. How about Verified by VISA that my and many, many other credit unions use? It's a simple process where if one places an order over the 'net and the transaction meets some fraud potential algorithm the transaction is run through Verified by VISA requiring an account and separate password. Such a step does much, much more to prevent fraud and identity theft than hundreds of millions of robocalls ever could.

My credit union didn't send out a breach notice on the Home Depot breach. My credit union received a list of possible compromised credit cards and issued new ones. There; problem solved without the need for millions of harassing "get in the face" breach notifications. Clearly, there are many solutions to the breach problem and most of them do not involve any automated phone calls to cell numbers.

ABA admits that all that breach robocalls can do is recommend: "...aggressive account monitoring to locate fraudulent activity..." Such robocalls are not proactive; they are reactive in nature and more CYA for the banks than help for the consumer. ABA's robocalls cannot return money that has already been taken fraudulently. But then consumers aren't responsible for loses that happen to banks with lax security. Consumer lose is limited in most case to $50.00. Consequently, these breach notifications will serve

no other purpose than a "get in the face" Customer Relationship Management[1] or CRM effort. It is ultimately nothing more than an advertising gimmick.

ABA engages in what can best be described as attempted hostage taking. ABA has already made clear to the Commission that if the Commission does not grant the "intended" called party petitions ABA members will refuse to provide services that consumers have requested. ABA makes the same "all or nothing" threat with their petition for exemption. Consumers and the Commission should not and cannot be held hostage by the banking institutions. Prior express consent has worked since the enactment of the TCPA. ABA has not provided any sound legal basis to do away with prior express consent. Threats, such as ABA makes, are not a valid legal basis to do away with prior express consent.

ABA's true colors emerge when ABA claims to know better than consumers what communications they want on their cell phones. What ABA intentionally ignores is the fact that cell phone service is not free. Even when messages are not individually charged to the consumer the consumer still pays for the service. Recent decisions from the courts have recognized this fact. See for example *Fini v Dish Network*, Case No.: 6:12-cv-00690 (M.D. Fal, 2013) holding that: "…Plaintiff and her husband **paid something** for her cell phone service…" See also *Lee v Credit Management*, 846 F. Supp. 2d 716. 729 (S.D. Tex. 2011) holding that: Lee has stated that **he pays a third-party provider for cellular phone services**." Consequently, unless ABA pays for cellular telephone service for consumers it cannot say with 100% certainty that breach, identity theft, remediation and bank transfer messages will not be charged to the recipient of the messages.

[1] CRM is also referred to as Customer Retention Marketing.

Whether someone is charged for a call or not should not be the only deciding factor on ABA's petition. One appellate court has made clear that autodialed calls are an intrusion on privacy: "…autodialed calls negatively affect residential privacy regardless of whether the called party pays for the call." *Osorio v. State Farm Bank, F.S.B.*, 746 F. 3d 1242 (11th Cir. 2014). Since autodialed calls "negatively" affect residential privacy then autodialed calls to cell phones obviously affect cell phone privacy much more.

Unlike the Cargo Airline Association ABA has never stated that it was working with wireless carriers to ensure that the breach, identity theft, remediation and bank transfer messages will not be charged to the recipient of the messages. Other than a cursory claim no evidence was provided by ABA to the Commission that ABA members are working with wireless carriers to ensure that recipients are not charged for the messages. But then what wireless carrier will offend its customer base because they cut a deal with banks and debt collectors to deliver Free to End User messages that their customers never requested? Again, until ABA members pay for consumer wireless service consumers will be charged in some way for ABA member breach, identity theft, remediation and bank transfer messages.

ABA has the gall to claim that allowing those that do not want the ABA member messages to opt out will: "…harm rather than advance consumer privacy…" There is nothing in the record or even in the history of the TCPA that opt out somehow "harms" consumers. It is a statement from the banking industry that considers consumer protection laws as an impediment to their greed. ABA's own comments clearly show the pervasive negative attitude of the banking industry towards consumer protection laws:

> "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."

The banking industry considers all consumer protection laws as being "…burdensome, unsuitable and inefficient…" This unacceptable attitude comes from an industry that is responsible for the recent economic downturn that led to millions losing their jobs and homes. This industry wants the Commission to believe they are on the side of the consumer. Nothing can be further from the truth!

As can be easily seen from the ABA petition and comments, the extremely small inconvenience of removing non-consenting recipient cell numbers from an autodialer list affects ABA member's greed too much. It is not so much a privacy issue as it is an issue of spending a few seconds removing a number which ABA members do not want to waste their time on. This refusal to remove non-consenting recipient cell numbers from an autodialer list is prevalent throughout the many TCPA claims filed in the courts today. See for example the Submission for the Record of the Coniglio v Bank of America NA matter. Even pro financial institutions commentors are against a no opt out scheme proposed by ABA. Nobel Systems Corporation admits that: "Merely because this may be a more efficient channel for the sender to use is not a sufficient reason to force the recipient to continue receiving such messages. At this point, the overall benefit does not justify the privacy intrusion." So even ABA's own camp admits that these breach, identity theft, remediation and bank transfer messages are an invasion of privacy when made without consent.

The Commission must not forget that this same industry is spearheading petitions to limit the definition of automatic dialer to exempt every dialer in use today. This same industry is also spearheading efforts to redefine called party to mean "intended" called

party despite the fact that dozens of district courts, two appellate courts and even the FCC have rejected such a nonsensical approach. This same industry is also spearheading efforts to hold that prior express consent cannot be revoked. In other words the banking industry has set its sights on total annihilation of any and all protections the TCPA has on calls to cell numbers.

ABA members do not have a constitutional right to consumer's cell phones. Transmitting a message to someone's cell phone without permission is a form of trespass to chattel. Consequently, the Commission cannot shield the banking industry from a common law tort claim. But the TCPA is, after all, a consumer protection statute and not a business protection statute. Consequently the Commission should strengthen not limit the TCPA when it comes to the millions of banking industry robocalls that violate the TCPA.

I suggest the Commission look at the federal docket for them to see how many TCPA claims have been filed against financial institutions. At least 90 percent if not more of all TCPA claims are against financial institutions and most involve calls to consumers that do not owe the debt[2]. And in most of those claims the calls are to numbers where consent never existed or was withdrawn. The Commission can see with its own eyes the track record of the financial institutions at thumbing their nose at the TCPA. It is no wonder that banks and debt collectors want to entirely neuter the TCPA.

A recent ex parte presentation by Wells Fargo is an eye opener. Wells Fargo has gone so far as to tell the Commission how it should influence jury's in reaching a verdict. Wells Fargo is so intent on neutering the TCPA that they are demanding that the

[2] http://www.allaboutadvertisinglaw.com/wp-content/uploads/sites/82/2014/12/TCPA-Update-11-24-14.pdf

Commission violate the constitution's separation of powers. The Commission can implement and clarify its rules. The Commission cannot influence a jury in such a way as to create a "good faith" defense for robocalls to cell phones where no such exemption exists in the TCPA.

The TCPA was enacted in response to the changes in technology that allow increased access to consumers. Today, the effectiveness of the TCPA can be measured by how effectively the TCPA protects consumers' cell phones. The greater number of calls received on a cell phone increases the likelihood that those calls will be received at a dangerous time (e.g., while driving a car[3]). Therefore, draconian interpretations that eliminate entirely prior express consent and the right to revoke consent must be rejected outright.

The Commission must bear in mind that the effectiveness of the TCPA will ultimately be defined by its ability to protect consumers' cell phones from automatically dialed calls made without consent. The Commission must also bear in mind that consumers are increasingly experiencing more illegal conduct on their cell phones from legitimate companies than by any other media. The banking industry is the biggest culprit of this illegal conduct!

The blame is put on the widening use of cell phones. Such blame is misplaced. It is the use of automatic dialing technology with inadequate calling procedures and a pervasive environment of industry indifference to consumer privacy and safety that is to blame.

[3] Many states have enacted laws that prohibit texting and calls while driving due to the distractions that the text and calls create.

ABA members already have what they want. They can transmit all the breach, identity theft, remediation and bank transfer messages they want as long as they have consent. Allowing ABA members to transmit their breach, identity theft, remediation and bank transfer messages to numbers never given to them is condoning an invasion of privacy on a massive scale. And no opt out makes the invasion of privacy even more intrusive. If the Commission grants the exemption many cell phone users will sour on the use of the new technologies afforded by smart cell phones.

No one likes spam messages. The Commission must not grant an exemption for banking industry spam messages. The Commission can and must deny the ABA petition.

Respectfully submitted,

_____/s/_____

Joe Shields
Texas Government & Public Relations Spokesperson for Private Citizen Inc.
16822 Stardale Lane
Friendswood, Texas 77546