Comment on AOR 2012-26

DB CAPITOL STRATEGIES

PAC • CAMPAIGN • NON-PROFIT • POLITICAL LAW

August 1, 2012

Anthony Herman, Esquire
General Counsel
Federal Election Commission
999 E Street NW
Washington, DC 20463

RE: Comment on Advisory Opinion Request 2012-26 (ArmourMedia, Cooper for Congress Committee, and m-Qube)

Dear Mr. Herman:

These comments are submitted on behalf of National Defense Committee Political Action Committee ("NDC PAC") in response to Advisory Opinion 2012-26 ("AOR") requested by ArmourMedia, Cooper for Congress Committee, and m-Qube (collectively, the "Requesters") regarding the implementation of cellular phone text messaging for contributions to political committees. For the reasons set forth below, we write to express our hope that a campaign contribution method similar to that detailed in the AOR can be implemented. However, the AOR should not be implemented without considering 1) the potential fraud and abuse that can occur where - unlike through the well-established and easily understood data treasurers receive through the banking system - treasurers will not be able to receive adequate information from carriers or aggregators on which to base their compliance duties and 2) the burdens this in turn imposes upon wireless carriers, aggregators and others.

Protecting the interests of service members

NDC PAC has a particular interest in matters effecting veterans and service members with respect to the electoral process, from voting rights to military readiness to Veterans benefits. NDC PAC believes that permitting campaign contributions via cellular phone text messaging has manifold benefits to the deployed service member community. Among them is the ability for deployed U.S. military to exercise their Constitutional rights, actively participate in the political process, and make their voices heard through contributions. The process of making a political contribution, which can be cumbersome and costly when one is deployed abroad, could be transformed into a simple, convenient process through a text message contribution system.

U.S. soldiers deployed abroad should be able to take advantage of a text message contribution system that is reliable, secure, verified, and transparent. To that end, we ask the Commission to allow a text message contribution system that ensures U.S. soldiers deployed abroad who use

both U.S. and foreign-based wireless service providers[1] will have the opportunity to make text message political contributions to candidates for federal office in a system that is **secure, legally compliant, and free from the potential for fraud and abuse** we identify below. We strongly urge the Commission to take sufficient time and engage a broad spectrum of interested parties and stakeholders to implement a thoughtful solution to ensure deployed service members are able to fully participate in the political process.

Treasurers Liability

From the outset, we agree with the Requesters that the responsibility for determining whether a contribution made by text messaging is from a prohibited source remains with the political committee and not the wireless industry and connection aggregators. Political committee treasurers have the responsibility to obtain the identity of contributors and prevent excessive and prohibited contributions. Advisory Opinion 1991-20 (Call Interactive).

Committee treasurers are personally responsible for the timely and complete filing of reports or statements and for the accuracy of that information. *See* 11 C.F.R. § 104.14(d). Committee treasurers are also tasked with obtaining the identity of contributors and with the prevention of excessive and prohibited contributions. *See* Advisory Opinion 1991-20 (Call Interactive). Because committee treasurers are personally responsible for verifying the accuracy of contributor information, we agree that wireless carriers and connection aggregators are not responsible for determining the eligibility of a particular contribution. Consequently, the transactional platforms developed to process such contributions that are selected by these Treasurers should adhere to clear guidelines for compliance such that Treasurers may be assured of fulfilling their legal obligations under the Federal Election Campaign Act.

Established norms for transacting contributions

Until now, the compliance liability imposed upon treasurers has occurred in an environment where the financial instruments - such as checks, credit cards, PayPal, Google and other online payment accounts tied to checking accounts and credit cards, or cash - and the transaction processes are well understood. With these payment methods, political committee treasurers can rely upon built-in safeguards such as payor names on check faces, or payor names on credit card accounts with FDIC-insured institutions with longstanding anti-fraud measures in place. For

[1] Due to greater affordability, many U.S. military personnel obtain cellular phone service through a foreign-based wireless service provider when they are deployed abroad. However, the text message contribution system proposed in the AOR could prevent such persons who use foreign-based service providers from making text message political contributions. This is an unacceptable conclusion for the men and women that protect our freedom.

Dan Backer, Esq.,
Principal Attorney, licensed in VA, DC
202.210.5431
DBacker@DBCapitolStrategies.com

209 Pennsylvania Avenue SE • Suite 2109
Washington, DC 20003
202-478-0750(fax)
www.DBCapitolStrategies.com

Stephen M. Hoersting, Esq.
Counsel, licensed in OH
937.623.6102
SHoersting@DBCapitolStrategies.com

these well-established payment methods, placing liability on the treasurer is reasonable because there are multiple means of verifying contributor identification in order to comply with the law. With the system proposed in the AOR, however, the Commission cannot be sure that m-Qube's suggestion of providing political committee treasurers with a list of aggregator information will prevent foreign national participation or excessive campaign contributions via common fraud techniques.

The Commission previously recognized the serious problem of impermissible contributions from foreign and other sources. *See* AO 2010-23 (CTIA - The Wireless Association). There the Commission rightly held that when questions are raised regarding the legality of a contribution, "it is incumbent upon the service provider to forward 'the appropriate information'" to the committee so that it can meet its legal obligations. *Id., citing* Advisory Opinion 1991-26 (Versatel). Thus far, committee treasurers have only had to ensure the legality of contributions by analyzing well-understood and verifiable transactions. In performing their statutory duties, political committee treasurers may reasonably rely upon information the banking and financial industries gather. However, with text message contributions, there is no such guarantee or system to rely upon that will allow the treasurer the ability to verify contributions and prevent fraud.

Potential fraud

We are concerned about potential fraud with regard to the text message contribution system proposed by the Requesters in the AOR. The attestations, the $50 cap, and the factoring arrangement will not prevent individuals from employing common fraud techniques to circumvent federal election law and regulation. According to the Federal Communications Commission's online cell phone fraud guide, cellular fraud is defined as the unauthorized use, tampering, or manipulation of a cellular phone or service and it is a big problem. The primary type of cell fraud is subscriber fraud and the cellular industry estimates it costs carriers more than $150 million a year. *See* Federal Communications Commission, Cell Phone Fraud Guide, http://www.fcc.gov/guides/cell-phone-fraud (last visited July 30, 2012). Subscriber fraud is where an individual uses fraudulently-obtained identification information and uses it to set up a cell phone account. We are concerned that the text message contribution system proposed in the AOR would be susceptible to similar fraudulent activities. It is entirely foreseeable that a dishonest individual could engage in subscriber fraud and subsequently make numerous unauthorized text message contributions, thereby undermining the integrity of the federal election system.

Dan Backer, Esq.,
Principal Attorney, licensed in VA, DC
202.210.5431
DBacker@DBCapitolStrategies.com

209 Pennsylvania Avenue SE • Suite 2109
Washington, DC 20003
202-478-0750(fax)
www.DBCapitolStrategies.com

Stephen M. Hoersting, Esq.
Counsel, licensed in OH
937.623.6102
SHoersting@DBCapitolStrategies.com

The Federal Communications Commission also identified another common cell phone fraud technique known as cell phone cloning. *See id.* In this scam, individuals illegally scan radio wave transmissions from cell phone subscribers for unique serial numbers contained in every cell phone. These serial numbers are intercepted and then copied to a new phone, known as the cloned phone, and the legitimate cell phone subscriber gets billed for the cloned phone's usage. This common fraud technique could easily be employed to make illegal political contributions via text messages. We are concerned that the text message contribution system proposed in the AOR does not safeguard against common cell phone fraud techniques like cloning.

Another potential area for widespread fraud is prepaid cellular phones, also known as pay-as-you-go phones and, more colloquially, "burner" phones. Unlike landlines and traditional cell phone plans, consumers are not required to reveal their identity when purchasing prepaid cellular phones, which are available for less than $20 at Wal-Mart. *See, e.g.*, Wal-Mart, TracFone Samsung S125G Prepaid Cell Phone for $9.98, http://www.walmart.com/ip/TracFone-Samsung-S125G-Prepaid-Cell-Phone-Bundle/20933059 (last visited July 30, 2012).

In recognition of the rampant problems with fraud and criminal behavior associated with anonymous prepaid phones, Senator Schumer (D.-NY) and Senator Cornyn (R.-TX) introduced the "Pre-Paid Mobile Device Identification Act" in 2010. *See* Ellen Nakashima, *New proposal would require identification to buy prepaid cellphones*, The Washington Post, May 26, 2010, http://www.washingtonpost.com/wp-dyn/content/article/2010/05/26/AR2010052603693.html. The proposal would have required consumers to present identification to purchase prepaid cellular phones. Sen. Schumer noted in the Washington Post at the time, "This proposal is overdue because for years, terrorists, drug kingpins and gang members have stayed one step ahead of the law by using prepaid phones that are hard to trace." *See id.* Although the bill did not become law, it raised public consciousness of the extensive issue of fraudulent prepaid cellular phone usage. The text message contribution system proposed in the AOR is vulnerable to similar abuses. We cannot foresee, under the proposed system, what would prevent an individual from purchasing multiple anonymous prepaid cellular phones and subsequently making numerous, repeated and illicit political contributions via text messages.

Yet another potential basis for fraudulent abuse of the proposed text message contribution system is the practice known as spoofing. *See* Federal Communications Commission, Cell Phone Fraud Guide, *supra*. Under this method, cellular phone users set who the sender of the text message appears to be and replace the originating cellular phone number with other text. Individuals wanting to spoof text messages may visit websites like FakeMyText.com, which offers "new, easy to use, anonymous and fun texting service," SpoofCard.com/sms, and

TextFromWho.com, which "provides a worldwide anonymous text service that allows our customers to send untraceable anonymous text messages to any cell phone, anywhere in the world." Software packages such as Clickatell, which provides commercial-grade bulk text messaging services, also offer the public tools for text message spoofing. The transmission of anonymous and untraceable text messages is a growing problem. The New York Times reported that American consumers received about 4.5 billion unsolicited text messages in 2011, more than double the total in 2009. *See* Nicole Perlroth, *Spam Invades a Last Refuge, the Cell Phone*, New York Times, April 7, 2012, http://www.nytimes.com/2012/04/08/technology/text-message-spam-difficult-to-stop-is-a-growing-menace.html. Text messaging is a realm plagued with fraud and we are concerned similar fraudulent behavior will hinder the integrity of federal elections. The text message contribution system proposed in the AOR would do nothing to stop unscrupulous individuals from spoofing political contributions and circumventing federal election law.

In addition, the identity of the contributor is not verified at the time the contribution is donated and made available to the campaign within 10 days through the factoring system proposed in the AOR. The lack of identifying information other than a phone number at the time the campaign contribution is made leaves open the possibility for unchecked fraud, including contributions by foreign individuals. There is also the risk that individuals on a "family," "business" or other "shared" cellular phone plan could make text message contributions unauthorized by the individual actually paying the cell phone bill. For example, with a family plan, the contribution could be made by a minor child, but the bill paid by a parent, a potential additional violation of 2 U.S.C. § 441f. A business plan could allow employees or business owners to make contributions on their employer-paid phones, additionally resulting in unlawful corporate contribution, made with pre-tax dollars.

In order to ensure the integrity of the process, it seems self-evident that substantially more research, analysis, discussion, and resulting guidance on the operation of a text message contribution system is absolutely necessary.

No harm from a thoughtful, deliberate process

Should the Commission take more time implementing this novel, never-before-used means of contributing, no individual wanting to contribute to a federal election campaign will have their First Amendment rights infringed because of a delay in the roll-out of a text message contribution system. Americans can currently donate to election campaigns through many payment methods such as mail, in person, or online. Since a rapidly growing percentage of cell phones have Internet access, many Americans can already make political contributions online using their cell phone. In early 2012, 88 percent of American adults have a cell phone and more

Dan Backer, Esq.,
Principal Attorney, licensed in VA, DC
202.210.5431
DBacker@DBCapitolStrategies.com

209 Pennsylvania Avenue SE • Suite 2109
Washington, DC 20003
202-478-0750(fax)
www.DBCapitolStrategies.com

Stephen M. Hoersting, Esq.
Counsel, licensed in OH
937.623.6102
SHoersting@DBCapitolStrategies.com

than half of these cell phone owners use their phone to go online - a jump of more than 23 percent in the last two years. *See* Pew Internet & American Life Project, Cell Internet Use 2012, http://www.pewinternet.org/Reports/2012/Cell-Internet-Use-2012.aspx (last visited August 1, 2012). For the small percentage of the population that uses prepaid phones and does not have a credit card, they may contribute via the U.S. Postal Service in amounts greater than the $50 cap proposed in the AOR.

To quickly approve the AOR on an expedited basis may open the federal election system to widespread fraud, abuse, and illegal contributions from unlawful sources. We believe that the Commission should consider these issues outside the rush of a twenty-day decision period, and most appropriately through a rulemaking. Accordingly, we urge the Commission to reach an outcome that ensures deployed U.S. military personnel may participate and engage in political speech via a text message contribution system once a legitimate system can be properly implemented. We also encourage the Commission to ensure that the text message contribution system is one that adequately protects against illicit contributions and fraud. We thank you for considering our viewpoint.

Respectfully submitted,

/s/
Stephen M. Hoersting

Dan Backer

William Atkinson

Dan Backer, Esq.,
Principal Attorney, licensed in VA, DC
202.210.5431
DBacker@DBCapitolStrategies.com

209 Pennsylvania Avenue SE • Suite 2109
Washington, DC 20003
202-478-0750(fax)
www.DBCapitolStrategies.com

Stephen M. Hoersting, Esq.
Counsel, licensed in OH
937.623.6102
SHoersting@DBCapitolStrategies.com