MYL PAC and MYL C4
% Nick Staddon, Secretary
122 Pinecrest Rd.
Durham, NC 27705

Federal Election Commission
Office of General Counsel
999 E Street, N.W.
Washington, DC 20463
ao@fec.gov

Re: AO 2013-15 Conservative Action Fund

November 16, 2013

Dear Commissioners:

Please accept this comment regarding AO 2013-15 Conservative Action Fund on behalf of Make Your Laws PAC, Inc. (MYL PAC) and Make Your Laws Advocacy, Inc. (MYL C4).

This comment supplements our previous comments, to address the issues discussed in the Commission's meeting on November 14th, as invited by the Chair Weintraub.

1. *Investments vs depreciating or constant-value assets*

Assets such as cases of paper, prepaid cell phones, computers, gift cards and frequent flier miles are either fixed in value, depreciate, or are worth less when converted to currency. They are also much harder to transfer anonymously *en masse* than Bitcoin.

We agree with Mr. Backer that it is entirely reasonable to permit PAC-to-PAC transfers of such non-investment, less easily abused assets without first requiring their liquidation.

Bitcoin, like stock, is not an ordinary asset of that sort. Given the very wide fluctuation in its market price, holding on to Bitcoin (rather than converting it immediately to currency) represents an *extremely* speculative investment.[1] Requiring the liquidation of investments — especially ones whose transfer is difficult to audit — would be entirely appropriate. The slight transaction cost is well worth the increase in transparency and decrease in financial speculation.

[1] Currently, Bitcoin markets are overwhelmingly dominated by speculation. Because there is not enough Bitcoin-denominated exchange of goods and services to form an adequate Bitcoin-only marketplace, Bitcoin users have to use currency to purchase most goods and services (e.g. a restaurant that accepts Bitcoin still has to pay its own suppliers with currency). This imbalance between Bitcoin's use as a speculative trading commodity and its use as a *bona fide* medium of exchange is what largely drives its market volatility.

If Bitcoin becomes *primarily* used as a bona fide medium of exchange — and in part, the Commission's decision about whether to permit PACs to purchase ordinary goods and services with Bitcoins will affect that — its market price volatility will go down, becoming more based on real value and less on speculation.

We suggest that investment vs non-investment assets, and traceable vs non-traceable assets, are two good ways that the Commission could draw lines between the kinds of in-kind contributions it discussed. We *don't* believe that tangible vs intangible is a useful distinction.

We would like to mention again that we *agree* with CAF that they should be permitted to purchase ordinary goods and services using Bitcoin, and to take advantage of merchant discounts for Bitcoin usage (which is a more efficient medium of exchange because it cuts out most of the intermediaries of current financial transactions).

It is also simply a technical *necessity* to disburse Bitcoin to anonymous third party Bitcoin miners (albeit in very small amounts) in order to conduct any Bitcoin based transactions. If the Commission forbids *all* disbursement of Bitcoins, it forbids all *outgoing* transactions of Bitcoins; any PAC that receives an anonymous Bitcoin contribution would be forced to choose between illegally possessing the Bitcoins or illegally disbursing them to an anonymous miner.

However, we do *not* believe it appropriate to permit a PAC to directly use Bitcoins to fund independent expenditures, FECA contributions, or any other things that deserve heightened scrutiny and traceability.

2. *Disclosure of PACs' Bitcoin addresses and transaction IDs*

If, against our advice, the Commission decides that PACs *are* allowed to transfer Bitcoins to recipients subject to heightened scrutiny, they should at the very least be required to adequately report such transfers — namely, to document the Bitcoin block chain transaction ID and the Bitcoin addresses of both the sending and receiving PACs. (This is *in addition to* all of the accounting standards that we proposed in section 1 part 5 of our initial comments.)

Without appropriate Bitcoin-specific transaction records, PAC transactions of Bitcoin would be completely unauditable.

3. *Contribution vs non contribution accounts*

As a hybrid Super PAC itself, MYL PAC must *strongly* disagree with Mr. Backer's claim that Super PACs are subject to any less scrutiny, public record, or public interest in disclosure. *All* contributions and expenditures that are used to influence elections have an extremely high bar for disclosure in the public interest. If anything, given that a Super PAC can receive *unlimited* contributions, it is *more* important that those contributions can be reliably traced.

If the Commission permits a Super PAC to receive Bitcoins without adequate protections, or *any* Bitcoin-derived contributions via a 501(c)4, it would create a giant loophole in the FECA that would permit unlimited, anonymous, foreign national sourced contributions to be used to

influence elections, which is completely unacceptable under *McConnell* (as we discussed in section 1 part 6 of our initial comments).

4. Identification of Bitcoin donors

As Mr. Backer mentioned, PACs are required to make a "best effort" to identify contributors, not to do so with absolute certainty. They are however *also* required to take reasonable precautions to deter unlawful activity, especially if they know something is liable to abuse. Our proposal in section 1 part 5 of our initial comments was based on and consistent with the Commission's prior rulings on this issue, and strikes an appropriate balance.

A PAC should be required to collect full information from the purported donor; the donor should be required to attest that the Bitcoins contributed belong to them and not to a third party; the amount contributed to a PAC (as opposed to a 501(c)4) should be limited to $100 when it is in a medium of exchange that has serious inherent problems with traceability (as is true of cash); Bitcoin-based contributions to a PAC should use the one-time linked-address method exclusively; and PACs should keep records of linked addresses & transaction IDs.

If a PAC fails to get adequate information on the donor, gets an unattributed contribution or a contribution outside of the one-time linked address system, or gets a contribution (or aggregate set of contributions) that is suspicious, the Commission should mandate that the PAC dispose of them to an entity permitted to receive unlimited anonymous contributions — and prohibit *all* Bitcoin refunds. Mr. Backer said that this is also what he would advise.

Mr. Backer's analogy to prepaid credit cards is apt in certain respects. Prepaid cards have *some* anonymity when purchased with cash. However, they can be traced at least to a specific store where they were bought, it's hard to buy *thousands* of dollars worth of prepaid cards with cash, and it's hard for someone overseas to send thousands of dollars (or hundreds of thousands, in the case of CAF's non-contribution account) using prepaid cards.

The degree of anonymity, laundering, and foreign sourcing possible with Bitcoin completely dwarfs what is possible with prepaid credit cards — even ones bought with cash — and that is where Mr. Backer's analogy fails. Bitcoins can be created by anyone in the world.[2] The end of an audit trail for a prepaid card is, at worst, a physical location and video surveillance; the end of a Bitcoin audit trail, even *with* our proposed accounting, is potentially nothing at all. There is *far* greater potential for abuse with Bitcoin than with prepaid cards, which is why we believe that Bitcoin contributions to PACs should be subject to the $100/yr/contributor/recipient limit.

There can and should be Bitcoin-specific accounting (just like there is check and credit card specific accounting) which creates at least some minimal degree of audit trail. We proposed

[2] A successful Bitcoin miner receives 25 bitcoins — currently worth ~$11,250 — and is virtually impossible to trace to an actual person if they take appropriate precautions for network anonymity.

appropriate methods in section 1 parts 5-6 of our initial comments.

5. *It is not possible to reliably refund Bitcoins to the control of the person who sent them.*

We addressed this repeatedly in our initial comments. The underlying Bitcoin protocol simply does not have a mechanism to reliably determine what address an incoming transaction originated from (it may originate from many addresses — or from none, if made by a miner). Even if it did, the address *sending* Bitcoins does not necessarily belong to the user *controlling* the transaction. If a Bitcoin exchange user buys bitcoins, it is the exchange's own wallet that sends them to whatever address the user specifies; "returning" the Bitcoins would give them to the *exchange*, not back to the originating user.[3]

In previous drafts of our initial comments, we tried to create *some* "safe harbor" scenario by which Bitcoins might be reliably refunded to their owner. Unfortunately, we discovered a way to easily subvert *all* such scenarios (even extremely restrictive ones). It is simply not currently possible to reliably "refund" Bitcoins to their original owner, and it probably never will be. Even the "refund" mechanisms being developed now rely on the original owner *designating* their desired refund-to address, which could actually be controlled by a third party.

6. *Mr. Backer is factually incorrect on several points:*
    a. It is not possible to reliably know what country a given Bitcoin user is from.
    b. It is not possible to refund, refuse, prevent, or screen Bitcoin contributions from an unwanted source.
    c. It is not possible to determine the contact information of a Bitcoin user, nor to even *verify* a contributor's claim that they own a Bitcoin address.[4]
    d. Bitcoins do not have a "serial number" like a dollar bill.
    e. Bitcoins do not all originate from a single computer; new Bitcoins originate from anonymous computers dispersed throughout the world, every few minutes.
    f. Bitcoins are not "stored value" denominated in US dollars; they are *traded for* currency on highly fluctuating open markets.

To explain why these are true, we need to give some more background on how Bitcoins work.

Technically, there *are* no "bitcoins" *per se*. The Bitcoin system has *addresses* (which are a type of public key[5]); *transactions* (which authorize the transfer of Bitcoins to whoever can prove they

[3] This would violate the FECA (by returning a contribution to a third party).

[4] It is *technically* possible for a Bitcoin user to cryptographically sign a statement of this sort, but this is completely outside the reach of all but very highly advanced users to either make or verify.

[5] http://en.wikipedia.org/wiki/Public-key_cryptography. Even more technically, a transaction can designate things other than a Bitcoin address as ways to prove that one is allowed to control the output of a

control a given public key); and *blocks* (which form the public history of the Bitcoin network by authenticating the previous block, any other transactions its miner wants to, and one transaction of 'new' Bitcoins that the miner gets for creating the block).

Bitcoins originate from a Bitcoin miner, in an amount and rate given by the Bitcoin protocol (currently 25BTC / block and 1 block every ~6 min). They are not actually a thing or number that is "transferred" from one computer to another. Bitcoin users sign transactions, and miners include those transactions in the public blockchain, all using public key cryptography. The *transactions* are transferred among the peer-to-peer network of Bitcoin users.

Anything that is included in a block (i.e. all transactions and all public keys that have been designated as receiving Bitcoins) is public knowledge. A Bitcoin user's "wallet" stores the *private* keys of a set of Bitcoin addresses (and a ledger of its transactions & current "balance" for user convenience), thus enabling the user to control whatever amount of Bitcoins that the history of previous transactions have credited to the associated *public* key.

It is simply by tracing the *entire* transaction history from its very beginning (i.e. dead reckoning) that everyone knows how many Bitcoins every address "owns". And while Bitcoin *transactions* are public, the *transactors* are not identified by *anything* other than by a cryptographic public key. The various methods for laundering Bitcoins try to ensure that even the public transactions do not reveal *actual* underlying exchanges of ownership.

Bitcoins are not atomic (unlike dollar bills), and do not have serial numbers. A transaction can be for any increment of 0.00000001 Bitcoins.[6] *Transactions* have ID numbers that are public.[7]

A Bitcoin user can control any arbitrary number of Bitcoin addresses. Many transactions transfer Bitcoins between multiple addresses simultaneously; there is no way to distinguish "which" address gave to which recipient. There is no easy way even to know reliably what set of Bitcoin addresses are controlled by a single person (without using sophisticated network traffic analysis — and even then, the conclusions are generally fuzzy at best).

Because transfers of Bitcoin are made based *only* on the authorization of the sender, not the receiver, it is not possible to "screen" or refuse an incoming transaction. Once the transaction to your Bitcoin address is signed by the sender and incorporated into the public blockchain, it is public knowledge that you own those Bitcoins, regardless of your consent. See section 1 parts 5-6 and section 2 part 3 of our initial comments for the policy implications of this.

Because the blockchain does not store IP addresses, and a computer *transmitting* a given

---

transaction (and this is how future improvements on Bitcoin are built, that would eg designate a "refund" address or "contracts"), but currently, a Bitcoin address is the overwhelmingly most common mechanism.

[6] Bitcoin is currently traded at ~$450 per 1 Bitcoin. It would be infeasible *not* to have fractional transactions, or to have a separate "serial number" for each hundred-millionth of a Bitcoin.

[7] E.g. http://blockexplorer.com/t/6DxJkqkhnP

transaction is not necessarily operated by the the user *initiating* that transaction, it is not possible to know the country of a Bitcoin user without doing sophisticated network traffic analysis.[8] Most Bitcoin clients have built-in support for the Tor anonymizing network,[9] which makes tracing the true source of a network request to its owner's IP more or less impossible.

7. *Separate schedule for in-kind contributions and assets*

We agree that it would be a good idea for the Commission to establish a distinct reporting method for in-kind contributions — and for that matter, for *all* assets owned by a PAC — which would be able to more clearly account for things such as appreciation, depreciation, re-investment, transaction records, type of asset, persistent asset identifiers, etc. that do not really fit in the current reporting forms.

We also agree with Mr. Backer that in the meantime, there should be a line item for the appreciation or depreciation in value of assets that are held.

8. *Re. the technological modernization notice of proposed rulemaking*

We believe it would be an *excellent* idea to include Bitcoin in the Commission's upcoming rulemaking on technological modernization.[10]

9. *Re. punting on implicit questions*

If the Commission's final AO on this matter punts on any of the questions that we have raised in our comments (re. accounting and information gathering standards, transaction limits, disbursements to bitcoin miners, valuation of Bitcoins having a higher cost to transact than they are worth, reporting of PAC-mined bitcoins, and contributions to/from 501(c)4s), we will have to immediately file an AOR to explicitly ask those questions — to ensure that there is a clear safe harbor policy for appropriate handling of Bitcoin contributions, together clear mandates for

---

[8] See http://www.slideshare.net/dakami/black-ops-of-tcpip-2011-black-hat-usa-2011 for an in-depth technical discussion by Dan Kaminsky, one of the leading experts in computer security. Again, this is an evolving area, with techniques being developed on both sides. However, it does not pass the simple test of being auditable by someone of ordinary technical skill vs someone using even moderately good precautions.

[9] https://www.torproject.org/about/overview.html.en

[10] If the Commission wishes, I would be happy to testify for its hearings therein. I believe that someone with my combination of technical background and campaign finance law knowledge could provide an unusual contribution by being able to bridge the often large divide between law and technology.

Helping with the NPRM would also align well with MYL's goals of systemically improving our political system through technological modernization.

appropriate, auditable accounting that are adequate to deter abuse.

We suggest that it would be more efficient (and easier on its already overburdened legal staff) for the Commission to address these issues now.

I realize that the above discussion of how Bitcoin operates is somewhat technical. I have tried to balance precision with understandability and explanation in terms of practical effects.

If you, your staff, or Mr. Backer have any questions or comments, please do not hesitate to contact me at sai@makeyourlaws.org or (717) 469-5695.

Sincerely,
Sai
President & Treasurer
Make Your Laws PAC, Inc.
Make Your Laws Advocacy, Inc.

P.S. Since Chair Weintraub mentioned that nobody present at the meeting had ever actually *used* Bitcoins, and even Mr. Backer seems to have several fundamental misunderstandings about how Bitcoin works, I feel I should mention my own background here.

I have personally used Bitcoin to pay for goods and services on multiple occasions; given a guest talk on Bitcoin and Tor based anonymous transactions to UC Berkeley Boalt law school Prof. Chris Hoofnagle's class on computer crime law; published independent research about machine learning based de-anonymization techniques[11] that directly contributed to fixing flaws in the technical standards of the World Wide Web Consortium; and worked in computer security and web development[12] for several years.

My comments about security issues with Bitcoin, and ways to address them, are based on my professional expertise, coupled with my legal knowledge of the FECA. (I am not a lawyer, but I did write the entirety of our initial comments, including all of the legal analysis and research therein.) I consulted with Bitcoin developers and computer security colleagues to find *any* way how the issues we raised might be overcome by less stringent means than those we proposed; we concluded that there were none. I also consulted with them on both our initial comment and this comment, to ensure their technical precision.

[11] http://s.ai/presentations/css%20history.pdf

[12] http://s.ai/work