



October 21, 2014

Dana Syracuse, Esq.  
Office of the General Counsel  
New York Department of Financial Services  
One State Street  
New York, NY 10004-1511

Dear Superintendent Lawsky and Mr. Syracuse,

This comment letter is submitted on behalf of BitGo, Inc. (“BitGo”) in response to the request for comment on the proposed Regulation of the Conduct of Virtual Currency Businesses specified in the Notice, 236 N.Y. Reg. 14 (July 23, 2014) (“Proposed Rule”) issued by the New York State Department of Financial Services (“NYDFS”).

BitGo is a Palo Alto, CA-based software company that has operated in the Bitcoin space since early 2013. We are recognized in the industry as the leading Bitcoin security platform and have pioneered industry-critical security technologies such as multi-signature, HD wallets. BitGo’s co-founders are veteran executives and entrepreneurs, and experts in digital currency, online security, and financial technology.

We have raised more than \$14 million in financing from venture capitalists, angel investors, and Bitcoin industry insiders who have backed successful companies like PayPal, Netscape, Red Hat, Proofpoint, Verisign, Juniper Networks, Yammer, and Tesla. We are a private company governed by a 7-person Board of Directors, including members who have served or currently serve on large public company boards.

We operate a software-as-a-service business model for enterprise customers. Our customers include exchanges, trading desks, hedge funds, family office investors, miners, e-commerce companies, non-profit organizations, and other businesses that hold Bitcoin in their treasury or use Bitcoin in their operations. We do not convert Bitcoin to or from fiat currency for our customers and we do not maintain custody and control of our customers’ Bitcoin holdings.

At BitGo, we believe that Bitcoin will change the world for the better. Bitcoin will usher in a new wave of financial freedom and global commerce. The vision we and other Bitcoin pioneers share will not come to fruition without the efforts of many, both startups and large organizations alike, having the freedom to innovate.

We understand and support the NYDFS’ stated mission is to protect New York consumers and national security, without stifling innovation, and we support

reasonable regulation to achieve those goals. However, in its current form, we do not believe the Proposed Rule will be effective.

We take very seriously the responsibility incumbent in us — as the leading brand for Bitcoin security and one of the top-funded companies in the industry — to share our perspective on the Proposed Rule in an effort to keep open the opportunities of innovation and entrepreneurship for all.

BitGo appreciates the opportunity to provide its comments on the Proposed Rule and thanks the NYDFS in advance for its consideration.

## **I. Overall Comments**

It is our view that the Proposed Rule will not be effective in its current form and would benefit from significant revisions and clarifications. While there are many areas of concern, this letter focuses on four key themes.

We support the comments published by policy and trade groups Coin Center, the Chamber of Digital Commerce, the Bitcoin Foundation, and the Electronic Frontier Foundation, as well as our industry peers Circle, Coinbase, and BitPay, among others. While each comment identifies different areas of improvement in the Proposed Rule, the collective mosaic of feedback is clear: more time is needed to get this right.

The themes on which we focus this comment letter are:

- (1) Acknowledge that Bitcoin existentially faces a dichotomy as (a) possibly one of the greatest technological and financial innovation in history, and (b) clearly in its nascent stage of development;
- (2) Focus efforts on empowering businesses, especially startups, to innovate and discover new and valuable use cases for Bitcoin;
- (3) Understand deeply the emerging standards and best practices that will make Bitcoin safer for businesses and consumers alike; and
- (4) Revise the Proposed Rule such that it (a) scopes to the realistic magnitude of risk, and (b) is distinct and consistent with existing federal and state regulations.

## **II. Bitcoin's Stage of Development and Appropriate Regulation**

Many analysts compare Bitcoin's current stage of development to that of the commercial Internet in 1993-1994. Bitcoin has achieved a high level of adoption and interest because the technology is novel and has inspired some of the brightest minds to dedicate the next phase of their careers and lives to it. But it is important to acknowledge that Bitcoin is still a very nascent platform and there is much work to do to make Bitcoin secure, scalable, and useful.

In the early days of the Internet, could we have imagined the scale of online commerce that Amazon.com, Google, and Apple would achieve? Could we have envisioned the powerful roles that Twitter and Facebook would play in transforming the political landscape of the Middle East? In 1993, a small number of people were just starting to get online. Today, there are more internet-connected mobile devices than there are human beings on this planet.

From a regulatory perspective, early Internet pioneers had the necessary freedom to operate and explore new business ideas. While there naturally was fear, uncertainty and doubt stemming from mainstream media coverage of the many bad things the Internet could be used for, entrepreneurs focused on building true and lasting value; and they were successful.

We can apply this same lens to Bitcoin. Bitcoin is a technology that is only 5 years old. The total market capitalization of all issued bitcoins is \$5.2 billion. And yet, the rate of Bitcoin-focused company creation and venture capital financing outpace that of the commercial Internet. If you plot these trends forward, Bitcoin will be more integral to our daily lives in another 15 years than we can possibly imagine.

With this in mind, what is the appropriate degree of regulation on Bitcoin businesses? We will explore specific critiques of the Proposed Rule and recommendations in the subsequent sections.

### **III. Startups and the Cost of Innovation**

To date, only 12 Bitcoin companies have raised funding in excess of \$10 million. I would argue that only these companies have the resources to comply with the requirements of the Proposed Rule, presuming a license was required for their business. Meanwhile, many other companies, especially software startups, would have no choice but to close up shop and exit the industry, or as some have suggested, ring-fence New York and exclude New York customers from Bitcoin innovation.

Either outcome would be tragic. BitGo does not support barriers to innovation such that only the top funded companies can operate in the Bitcoin industry.

In the Proposed Rule, there are numerous costs of compliance, both direct and indirect, including but not limited to:

- License application fees and procedures, e.g., fingerprinting
- Staffing of required personnel, e.g., CISO
- Background investigation reports
- Preparation of audited financial statements and pro forma statements
- Maintaining of books and records for 10 years
- Legal costs to manage all of the above
- Unspecified costs determined at the discretion of the Superintendent

Some comments have suggested the creation of a “safe harbor” provision to provide an onramp for startups until they reach a scale where they can afford to comply. While this is a reasonable compromise, even a safe harbor is not sufficient.

We recommend that the NYDFS review the merits of each of the direct and indirect costs associated with the Proposed Rule, and revise the requirements to include only those that truly meet the Department’s stated purpose of protecting consumers and national security.

In addition to the startup costs, the conditions put forth in the Proposed Rule on change of control will have a chilling effect on new company creation. Venture capitalists invest in companies that they believe will generate the best returns for their limited partners. Any regulation that inserts itself in the M&A flow will create a perceived discount on exit value, which means fewer companies will get funded and valuations will be lower.

We recommend that Section 200.11 be eliminated from the Proposed Rule. Instead, the NYDFS can require change of control notification, after which the NYDFS may review the validity of any Licensee vis a vis the then-current Proposed Rule.

We acknowledge Mr. Lawsky’s recent comments regarding the intention to not regulate software companies and we look forward to seeing that revised language for the Proposed Rule.

#### **IV. Emerging Standards and Technologies**

There are emerging standards and technologies that will ensure the security, privacy, and reliability of commercial Bitcoin use. It is critical that the Proposed Rule be future-proofed for these standards.

##### Multi-Sig (BIP32)

Multi-sig is the digital equivalent of a safe deposit box. Instead of using a single private key to transact, multi-sig wallets require multiple signatures from keys generated and held by multiple people, or in some cases, multiple institutions. This distribution of keys, when implemented properly, ensures that there is no single point of failure like we have seen with single-key cold storage implementations.

Multi-sig is enabled by a Bitcoin protocol standard called BIP16/P2SH, which was introduced in April 2012 and first pioneered commercially by BitGo in August 2013. Since that time, many leading companies are embracing multi-sig as a standard, including BitPay, Circle, Coinbase, and others.

Multi-sig also changes the classic definition of a “custodian.” With single-key Bitcoin storage, a custodian is one who holds the key. With multi-sig, the blockchain itself is the custodian and multiple parties need to cooperate in order to transact.

In the Proposed Rule, Section 200.2(n)(2) defines *Virtual Currency Business Activity* to include “securing, storing, holding, or maintaining custody or control of Virtual Currency on behalf of others.” With the advent of multi-sig, software companies providing security solutions, but not maintaining custody or control of Virtual Currency, should be exempt from the Proposed Rule. Therefore we recommend that Section 200.2(n)(2), and related sections of the Proposed Rule, be reworded to read “maintaining custody and control of Virtual Currency, and having contractual authority to initiate transactions, on behalf of others.”

### HD Wallets (BIP32)

Hierarchical deterministic (HD) wallets is an emerging standard defined in BIP32 that enables financial privacy on the public blockchain.

Maintaining privacy of transactions is a key tenet in building a robust financial network. Due to the blockchain’s public nature, specific actions need be taken to protect Bitcoin transactions and balances from being exposed. Users can accidentally reveal information about themselves and their past transactions if they use a single address for all of their Bitcoin activity, which has historically been the default behavior of most Bitcoin wallets.

For instance, imagine you work at a company that pays its employees in Bitcoin. You would of course know the address that is generating the transaction that pays you, and because the blockchain is public, you could also see the other transactions that address sent out into the network. This could allow you, or anyone else who knows the source address to infer sensitive information such as colleagues’ compensation.

HD wallets use cryptographic key derivation to manage multiple keypairs with a single secret seed. Every time a transaction is made with an HD wallet, the wallet service provider can rotate the address of your wallet so the outside world thinks it’s a new account; however, you don’t need new private keys for this account because the new keys are derived from your HD keychain.

At BitGo, we are proponents of privacy, not anonymity. We do not endorse the use of Bitcoin for illicit or nefarious purposes. We do, however, believe it is essential that the financial privacy of consumers and institutions be protected to the fullest extent possible.

The Proposed Rule introduces new risks to privacy breaches by requiring every Licensee to maintain records that include personally identifiable information, such as physical addresses for every transaction, as described in Section 200.12(a)(1).

Simply put, if JPMorgan Chase, Home Depot, and Target cannot safeguard consumer private data, how can we expect every Licensee to do so? Data security is ensured by compartmentalization. For example, the PCI Security Standard allows e-commerce companies to accept credit card payments while ensuring that these same companies do not store all pertinent credit card details that could be stolen by a hacker.

To bridge this example to the Bitcoin ecosystem, a payment processor and wallet operator need not know physical addresses of each party in a Bitcoin-to-Bitcoin transaction. Physical addresses, used for KYC compliance, are validated at the end points where financial institutions convert digital currency to fiat currency. Requiring redundant checks at every link in the value chain makes the overall ecosystem less secure for consumers.

### Standards Emerge from Within

Multi-sig and HD wallets are two examples of standards that have emerged from within the community of Bitcoin developers because they experienced first-hand the need for better approaches to security and privacy.

These types of standards are created when entrepreneurs have freedom to experiment with new ideas. Burdensome and costly regulation stifles this potential innovation because startups cannot afford to experiment, and ultimately consumers and businesses are worse off.

Let's look back at an example from the development of the Internet. Today, nearly every major website URL starts with "https". When you add in the "s", your Internet communication is being secured with TSL/SSL. But in the early days of the Internet, we did not have these standards. In fact, SSL was originally developed by Netscape and was not released publicly until version 3.0. Once SSL became a standard, and companies like Verisign integrated additional security procedures and technologies, the Internet became safe for e-commerce and experienced incredible growth.

What would have happened if, in 1994, a state regulator had required all Internet companies to use a secure network protocol that was underdeveloped and not ready to scale? There would have been less incentive for Netscape, Verisign and other industry members to band together behind SSL, and Internet commerce would have been less secure.

We recommend that the NYDFS conduct a thorough examination of the Bitcoin standards that have emerged, as well as those on the horizon, in order to inform revisions to the Proposed Rule.

## **V. Consistency with Other Regulation**

In reviewing the comments published by Bitcoin industry leaders and policy groups, many have pointed out both overlaps and inconsistencies between the Proposed Rule and New York Money Transmitter Requirements as well as federal regulation.

We agree with these assessments and recommend that the NYDFS review and revise the Proposed Rule such that it is (a) no more burdensome than existing regulations, and (b) absolutely clear which types of businesses are subject to the Proposed Rule, which are subject to New York money transmitter requirements, and which are exempt from both.

## **VI. Conclusion**

BitGo thanks the NYDFS for its efforts in attempting to establish the Proposed Rule, and we applaud the NYDFS for soliciting and listening to comments from experts and operators within the industry.

The NYDFS has an opportunity to demonstrate leadership among its state regulator peers in the United States by establishing a framework that encourages innovation in the digital currency industry while ensuring reasonable protections that are both consistent with other regulation and appropriate for the current stage of Bitcoin's development.

The NYDFS also has a unique position to aid in building a bridge between the existing financial capital of the world, New York, and the emerging global financial innovation rapidly developing in the Bitcoin ecosystem. Any regulation that causes leading Bitcoin companies to exclude New York customers from their services would be a failure of historic proportions.

We strongly encourage the NYDFS to not finalize the Proposed Rule until the concerns expressed in the many comments it has received have been satisfied. We look forward to revisions and further discussion on the Proposed Rule, and we stand ready to discuss any of the above comments with the NYDFS in more detail.

Sincerely,

A handwritten signature in black ink, appearing to read "Will O'Brien". The signature is fluid and cursive, with a long horizontal stroke at the end.

Will O'Brien  
CEO & Co-Founder  
BitGo, Inc.  
[www.bitgo.com](http://www.bitgo.com)