

Benjamin M. Lawsky
Superintendent of Financial Services
Department of Financial Services
One State Street
New York, NY 10004
October 21st, 2014

Dear Superintendent Lawsky:

This letter is submitted on behalf of Novauri LLC (Novauri) in response to the BitLicense regulations proposed by the New York Department of Financial Services (NYDFS).

ABOUT NOVAURI

Novauri is a virtual currency startup based in Denver, Colorado and San Francisco, California. Novauri will allow bitcoin users to purchase and sell bitcoin using ACH debits and credits from their bank accounts. The service will be available initially to US consumers in early 2015.

We are different from our competitors in that Novauri will not control the private keys to our customers' bitcoin addresses. Not only will Novauri never have access to customers' private keys, but our systems are designed so we will never see private keys in unencrypted form.

We intentionally built this feature into our service as a risk protection measure for our customers. Novauri cannot suffer from the catastrophic failures and massive internal thefts we've witnessed at services that pool customer bitcoin and control their private keys because Novauri never has control of our customers' funds, bitcoin or US Dollars. We feel strongly that this feature is both safer for our customers and cheaper for us as a service provider. Our design requires no expensive security layers around pooled wallets, no insurance for massive, pooled wallets that are vulnerable to insider theft, or regulatory responsibility as a fiduciary holding retail customer deposits like a bank.

INNOVATION, BITCOIN, AND CONCERNS ABOUT THE PROPOSED RULES

We believe bitcoin and its underlying blockchain technology is the most significant invention of the century. Bitcoin allows for unique digital information that can exist safely on the open Internet without the protection of a central authority. Bitcoin's unique combination of cryptography and "hashcash"-based proof of work consensus

with an integrated economic incentive to participate in the consensus that also creates an automated, and fully predictable monetary policy is something we've never dreamed of before 2009. The applications for this technology extend far beyond payment systems, and have the capability to uniquely identify anything digitally; a possibility that becomes exponentially more exciting when it intersects with other emerging technologies, such as the Internet of things, drone applications, or holograph-based UI and peer-to-peer communications.

That being said, the proposed regulation falls short in three key areas:

1. Redundancy with existing regulation, and creates unfair playing field,
2. KYC provisions and ineffective cybersecurity provisions are dangerous for consumers, and
3. Failure to create a risk-based system that scales with the risk of the service.

1) REDUNDANCY WITH EXISTING REGULATION, AND CREATES AN UNFAIR PLAYING FIELD

Novauri believes that the BitLicense regulation is written in such a way that it will greatly stunt growth and drive innovation to other States or Countries entirely. The regulation contains provisions that exclude existing banks from the rules entirely. The regulation then goes on to require (but not for banks):

- Data retention periods exceeding those required by banks of 10 years. This is longer than the 7-year period mandated by Sarbanes Oxley and the 5-year period mandated by the Bank Secrecy Act--measures that already apply to virtual currency businesses.
- Identity validation not only on the customer (required for banks), but on anyone interacting with the customer (technically impossible and not required for banks).
- Mandatory positions already required by other regulations.

Novauri recommends removing the provisions that exempt banks entirely, and replacing the redundant and overreaching language in these areas with a simple statement: The rules and regulations applying to bitcoin at a Federal level (especially from FinCEN) shall apply to all applicable virtual currency businesses with activities in New York State.

2) KYC PROVISIONS AND INEFFECTIVE CYBERSECURITY PROVISIONS ARE DANGEROUS FOR CONSUMERS

Perhaps the most dangerous aspects of the proposed regulations are the identity verification processes. We've already seen the disasters that the data retention provisions in the Bank Secrecy Act have caused in terms of the ongoing identity theft epidemic. Every week another bank is hacked, and more and more personal information goes up for sale on the darknet. We feel that these issues are an unintended consequence of the data retention requirements in the BSA, as well as the decision by certain companies to monetize "big data". Novauri feels that these are misguided regulations and business decisions, and is vehemently opposed to corporations storing and selling personal information. The economic costs of identity theft greatly outweigh any advertising revenue made by these companies, and the cost to taxpayers in reimbursing billions and billions of dollars in stolen tax refunds each year, to say nothing of the stress these unintended consequences cause normal people when they discover their identities have been stolen. This issue will be far worse with bitcoin, which features a public ledger. As soon as personal information is leaked, it can be associated with the blockchain and the entire financial history of individuals will be viewable by anyone. As written, Novauri feels the proposed KYC provisions in the BitLicense proposal constitute a potential threat to our National security.

Novauri recommends that the NYDFS delay the requirements around KYC until a more elegant solution evolves that doesn't risk massive identity theft incidents or violations of personal privacy. For the time being the BSA already requires customer identity verification over \$3000 daily, so the proposed regulation is redundant and unnecessary. When it is possible to synchronize national and state level regulation, Novauri recommends monetary penalties in lieu of criminal liabilities, but also revisions that better balance the individual right to privacy with the needs of law enforcement. Such revisions must include checks and balances that are non-existent today.

Furthermore, the regulation prescribes cybersecurity measure specifically. This is ineffective, as technologies are continuously evolving. Novauri recommends that the NYDFS require businesses that act as fiduciaries for customer deposits to hold deposit insurance for 100% of the value of all fiat and virtual currency deposits. If the business has faulty security, the insurance company can make that determination and increase their premiums. In the event that the business's security is unsafe, the insurance companies will not issue insurance at all. This is a "future proof" way to ensure

cybersecurity without politicizing the topic or risking that rules and regulations become ineffective and anachronistic with time, as they almost certainly will as written.

3) FAILURE TO CREATE A RISK-BASED SYSTEM THAT SCALES WITH THE RISK OF THE SERVICE

The proposed regulation doesn't differentiate between businesses that exchange fiat for bitcoin while taking control of deposits, those that exchange fiat for bitcoin and do not take control of deposits, or even businesses that exchange no currency at all and have no responsibility as a fiduciary. This will effectively kill all small businesses and startups in the State of New York, and if these rules are used as a model in other States, will drive the industry offshore entirely.

Novauri recommends creating at least two types of businesses under the proposed BitLicense regulation:

1. Virtual Currency Retail or Investment Banking Provider
2. Virtual Currency Retail or Exchange Service Provider

Virtual Currency Retail or Investment Banking Providers would be regulated in a manner similar to banks. These businesses should be required to hold deposit insurance that covers the full value of all fiat and virtual currency deposits. This insurance must cover not only "hot" wallets, but also "cold" wallets. The regulations should require businesses to digitally sign and prove bitcoin balances, and mandate verifiable third-party audits on the fiat side simultaneously to prove overall reserves matching customer deposits. Fractional reserves should be banned and carry harsh criminal penalties if an event resulting in a business operating on a fractional reserve basis is not disclosed immediately. This is critical from a consumer protection perspective in order to prevent the types of catastrophic failures we've seen at similar services in the past. Novauri also feels that the practice of "naked shorting" or the creation of other synthetic derivatives that do not require the issuer to hold actual bitcoin in reserve should not be allowed.

Virtual Currency Retail or Exchange Service Providers would be subject to minimal regulation. Because these businesses do not control customer deposits, the risk of a catastrophic failure is much lower, and such a failure would not result in the loss of customer funds. Any KYC validations required from the exchange of bitcoin for fiat would still apply as required by the Treasury, but insurance or excessive cybersecurity

provisions would not. Again, Novauri highly recommends using insurance as a way to “future proof” the areas of cybersecurity and KYC provisions.

In closing, given the possibilities presented by this emerging technology, Novauri requests that the NYDFS consider revising the rules heavily, adopting a progressive and risk-based approach that uses insurance in lieu of prescriptive measures, removes duplicative rules and regulations, and gives the technology the room it needs to grow and evolve.

Sincerely,

Will Madden
Founder & CEO
Novauri, LLC