Comments to the New York Department of Financial Services on the Revised Virtual Currency Regulatory Framework

Peter Van Valkenburgh & Jerry Brito

New York Department of Financial Services
Submitted March 27, 2015

Introduction

In revising the first draft of its Virtual Currency Regulatory Framework ("the BitLicense") the Department of Financial Services ("the Department") has shown a willingness to embrace challenge that should be celebrated. This new draft clearly indicates that the many comments submitted in the previous comment period were carefully reviewed and considered. We welcome this second opportunity to comment in the hopes that some further adjustments may ensure that New York State becomes a leader in the financial technology of the future.

Coin Center is an independent non-profit research and advocacy center focused on the public policy issues facing cryptocurrency technologies such as Bitcoin. Our mission is to build a better understanding of these technologies and to promote a regulatory climate that preserves the freedom to innovate using blockchain technologies. We do this by producing and publishing policy research from respected academics and experts, educating policymakers and the media about blockchain technology, and by engaging in advocacy for sound public policy.

We are not a trade association nor an industry group, and the comments that follow do not represent the views of any particular affected party. Our interest is helping the Department meet its public interest goals while ensuring that its policies do not inadvertently hamper the potential of blockchain innovation.

Each section of this comment outlines a specific change to the text of the regulation and offers supporting arguments and relevant background information. They are as follows:

1. **The definition of Virtual Currency Business Activity should be refined.** The words "storing" and "holding" should be removed and "maintaining custody or control" should be defined as: "having the ability to unilaterally execute or prevent a virtual currency transaction." Activities not aimed at retail-level consumers, *i.e.*

business to business services, should be exempted. Administering, controlling, and issuing a virtual currency should only require licensure if that currency is centralized by design.

2. **To protect the ability of small entrants to innovate, the Department should adopt an on-ramp for startups.** Firms dealing in less than $5 million in virtual currency annually should not be required to seek licensure. This exemption could be further conditioned on: (1) the business must register with federal money laundering authorities, and (2) must clearly disclose their conditional status to consumers. Firms with pending applications could also be offered a safe harbor, allowing them to operate while their license applications are pending; these transitional firms should similarly be registered with federal authorities, make clear disclosures, and if transacting greater than $5 million annually they can be required to post a standard bond pegged to the volume of business that they do.

3. **The Department should require notification of a new product or service rather than pre-approval.** A licensee should be required to alert the Department of new or changed plans, yet be left free to execute these changes or bring new products to market during a grace period, while the Department determines if capital requirements need to be adjusted or if the new plan simply cannot be offered to New York customers.

4. **The Department should make clear that virtual currency businesses do not need to acquire both a money transmission license and a virtual currency license.** The Department should grant BitLicenses by accounting for any and all assets and liabilities internal to the licensee, whether related to virtual currency or fiat currency custodianship. This inquiry should not be needlessly divided into two separate applications and investigations for licensure.

5. **The Department should eschew a new state-based anti-money-laundering program.** At the very least, the BitLicense's AML requirements should not go beyond Federal requirements under the Bank Secrecy Act. Proof of compliance with federal standards should satisfy a licensee's obligations under the BitLicense.

6. **So long as they comply with the recordkeeping and reporting requirements of the BitLicense, Virtual Currency businesses should not be liable when they or their customers obscure their identities while using Virtual Currencies.**

We thank the Department for this opportunity to comment, and hope you find this submission useful.

1. The Definition of Virtual Currency Business Activity Should be Refined

Custody, Control, Storing, Holding

The revised BitLicense includes the following in its definition of virtual currency business activity at 200.2(q)(2):

> storing, holding, or maintaining custody or control of Virtual Currency on behalf of others;

While we are grateful to the Department for removing "securing" from its latest draft, we remain concerned that this section remains vaguely drafted and could be interpreted as including businesses that the Department would not want to include as licensed entities.

As drafted, it is unclear what the two terms "storing" and "holding" actually mean, or what they add to the definition. Virtual currency is not, by definition, something that is capable of being held. Moreover, while we talk of storing files, perhaps in a cloud service like Dropbox, we cannot talk of storing Bitcoins. Bitcoins are not files; they are assignments of value made to pseudonymous addresses and listed on a public ledger called the blockchain. ***No one holds or stores bitcoins; one holds or stores the cryptographic keys that grants one permission to sign for transactions involving particular addresses***. In contrast, the second part of the Department's definition—"maintaining custody or control"—hits this mark. To the extent anyone ever *holds* or *stores* or, simply, *has* bitcoins it will be because they *maintain custody or control* over these cryptographic keys. "Storing" and "holding" are, therefore, confusing surplusage in the definition and should be removed.

We believe that the Department intends "virtual currency business activity" to encompass the activities of any entities that can misspend, lose, or fail to protect the customer funds with which they were entrusted. We believe the Department is justified in seeking that coverage. To be certain that the definition includes these parties after "storing" and "holding" are removed, we suggest that the department also define, "maintaining custody or control" as follows:

> *Maintaining Custody or Control* means having the ability to unilaterally execute or prevent a virtual currency transaction.

The only parties who are truly capable of harming virtual currency consumers are those who can lose, misspend, immobilize, or fail to protect a customer's funds. As the the Conference of State Bank Supervisors explains in its Policy on State Virtual Currency Regulation, "Such financial transactions or services place the activity provider in a position of trust. This position of trust is the basis for most financial services laws and regulations, and should be applied regardless of the medium of value."[1] Therefore, the parties that should be clearly

[1] Conference of State Bank Supervisors, *CSBS Policy on State Virtual Currency Regulation* 2 (Dec. 2014) *available at*

covered within the definition of virtual currency business activity are those who have the ability, ***on their own and without seeking additional information from the consumer***, to execute or prevent a virtual currency transaction. That ability raises the potential for virtual currency mismanagement and is what gives rise to a position of trust.

Some parties may have only one of several keys necessary to execute a virtual currency transaction. For example, if three key signatures are required to transact, and a service provider only ever holds one key, that service provider should not be understood as having *custody* or *control*. Minority key-holders cannot, solely by their own negligence or malevolence, lose consumer value. This is why our proposed definition includes the word ***unilaterally.*** That caveat is important. These parties can play highly valuable consumer-protective roles in the virtual currency ecosystem. They should be supported in their development by New York. Moreover, if they cannot abscond with or otherwise lose a customer's funds they should not be subject to the costly burden of licensure.

A company could, for example, help store only the disaster relief key of a customer who is afraid of losing her password or of her virtual currency exchange being compromised. Another company could, for example, hold a single key to sign off on transactions initiated using the consumer's key after, and only after, the company verifies that the consumer's phone has not been hacked or her key otherwise compromised.

Both of these hypothetical companies would provide an essential service in securing and safeguarding customer funds. Both hypothetical services are novel and unavailable to the customers of traditional banks and money transmitters because they rely on the use of new cryptographic tools and the blockchain to divide control between multiple businesses without using law to enforce that division. Neither of these companies, however, should need to be licensed as virtual currency businesses. Without possession of *sufficient* keys to move or immobilize the customer's funds on its own, the company does not pose a consumer protection risk; quite the opposite, they mitigate that risk.

These companies will be highly valuable innovators in the field of virtual currency. The technology that enables divided key control, called multi-sig, is widely understood within the industry as the single best tool for preventing a Mt. Gox-style heist before it even happens.[2] By defining custody and control to only extend to those who can ***unilaterally*** *execute a transaction,* the Department would send a credible and welcome signal to innovators in the virtual currency space: *New York values your effort to build technology that will compliment our consumer protection efforts and does not want to impede your progress unnecessarily*.

---

http://www.csbs.org/regulatory/ep/Documents/CSBS%20Policy%20on%20State%20Virtual%20Currency%20Regulation%20--%20Dec.%2016%202014.pdf.

[2] *See* Ben Davenport, *No Sleep Till Multi-Sig* (Jan. 12, 2015) https://medium.com/@bendavenport/no-sleep-till-multi-sig-7db367998bc7

A Business to Business Exception

As the Bitcoin ecosystem has matured, a new class of service providers has emerged. Interacting with the Bitcoin protocol can be technically complex, particularly when using advanced transactions such as the multi-sig or divided key transactions described in the previous section. Early bitcoin hosted wallet providers and exchanges generally coded these transactions in-house. However, this activity may not be the organization's expertise or comparative advantage. A consumer-facing business may find it more advantageous to focus on marketing, user experience, and regulatory compliance. They may, therefore, choose to contract-out the safekeeping of customer bitcoin keys to business-to-business firms that have developed expertise at utilizing multi-signature transactions and cold storage in order to best secure sensitive data.[3]

This is not novel in the world of Internet technologies. The video-on-demand service Netflix, for example, does not actually build or maintain the technology necessary to store video data. Instead, it relies on Amazon's cloud storage solution Amazon Web Services.[4] If a Bitcoin bank or exchange decided to contract-out the safekeeping of customer keys, it would raise a novel regulatory question. Do both the consumer-facing bitcoin business, as well as the service provider it uses to secure its data, need to be licensed? Double-licensing would substantially erode any cost-savings thanks to firm specialization, and would likely discourage a competitive market for business-to-business virtual currency security. The result would be higher fees for consumers as well as less security.

As a result, only one party should be licensed in such a situation: the consumer-facing business. The consumer-facing business holds itself out as a trusted intermediary to its customers who may not have the time, expertise, or caution necessary to effectively comparison shop or hedge against risks. A business-to-business Bitcoin firm, on the other hand, offers its security services to savvy institutions who have both the motivation and the capacity to aggressively comparison shop. In short, while market failures may prevent competition from effectively protecting individual consumers, a competitive market unfettered by regulatory costs in the business-to-business arena would best enhance security. Moreover, as long as the consumer-facing business is a regulated entity, the protections of the BitLicense will remain in effect for consumers.

Such a carve-out has been the longstanding norm for companies that are the legal agent of licensed money transmitters.[5] Similarly, the the Financial Crimes Enforcement Network

---

[3] Cold storage involves placing the majority of an institution's private keys in offline media, either disconnected computer memory like a thumb-drive, paper, or as memorized passphrases—a so-called brain bank. If keys are not stored on Internet connected servers, then they can only be accessed by compromising either the individual with access to the key or the physical security surrounding the key. The attack surface could thus be minimized by limiting the number of employees with knowledge of or access to offline key storage, and storing the offline drives or slips of paper in safe-deposit boxes or guarded premises.

[4] Amazon, *AWS Case Study: Netflix*, http://aws.amazon.com/solutions/case-studies/netflix/

[5] *See* New York Banking Law § 641 ("[N]or shall any person engage in such business as an agent, except as an agent of a licensee.").

("FinCEN") exempts merchant processors and banking intermediaries from duties under the Bank Secrecy Act because these entities are merely intermediaries between banks, which are heavily regulated entities.[6] FinCEN also exempts those who only provide "the delivery, communication, or network access services used by a money transmitter to support money transmission services"[7] The BitLicense should include a similar exemption in order to promote the development of enhanced security tools and services:

> Providing data storage, infrastructure, or security services, including the storage of data essential to transacting in virtual currency, to a licensed virtual currency business does not in and of itself constitute virtual currency business activity.

Controlling, Administering, Issuing

In public statements the Superintendent has been abundantly clear that he does not intend the BitLicense to require licenses of individuals or companies that only mine a decentralized digital currency, such as Bitcoin, or develop the software that underlies those currencies. As he recently stated:

> We are regulating financial intermediaries. We are not regulating software development. To clarify, we do not intend to regulate software or software development. . . . Mining per se will not be regulated. To the extent the miner engages in other virtual currency activities, however—for example, hosting wallets or exchanging virtual currency—a license may be required for those activities. For mining itself, there will be no license requirement.[8]

We strongly support the Superintendent's position. However, the recent BitLicense draft remains ambiguous as to whether the definition of virtual currency business activity encompasses mining and software development. Much is left to interpretation. The revised draft includes the following in its definition of virtual currency business activity at 200.2(q):

> "(5) controlling, administering, or issuing a Virtual Currency."

One can control, administer, and issue *centralized* virtual currencies. It is questionable whether anyone can be said to control, administer, or issue a *decentralized* currency. However, a future regulator interpreting 200.2(q)(5) may believe that definition does demand licensure of developers and miners as controllers, administrators, or issuers of decentralized virtual currency.

---

[6] 31 C.F.R. § 1010.100(ff)(5)(ii) ("The term "money transmitter" shall not include a person that only: . . . (B) Acts as a payment processor to facilitate the purchase of, or payment of a bill for, a good or service through a clearance and settlement system by agreement with the creditor or seller; (C) Operates a clearance and settlement system or otherwise acts as an intermediary solely between BSA regulated institutions.").
[7] 31 C.F.R. § 1010.100(ff)(5)(ii)(A)
[8] Benjamin M. Lawsky, *Excerpts From Superintendent Lawsky's Remarks on Virtual Currency and Bitcoin Regulation in New York City* (Oct 14, 2014) *available at* http://www.dfs.ny.gov/about/speeches_testimony/sp141014.htm

Centralized virtual currencies are created and controlled by a singular authority, usually a business. For example, Amazon.com has created Amazon Coin to allow its users to buy digital content on its sites.[9] Such a business can create digital tokens and distribute or sell them to customers. They can peg the value of the currency by promising to redeem those tokens for a fixed amount of fiat currency or some item of value, or they can allow the value to float according to market supply and demand. As the Financial Action Task Force ("FATF") has explained, "the vast majority of virtual currency payments transactions involve centralised virtual currencies. Examples [include] E-gold (defunct); Liberty Reserve dollars/euros (defunct); Second Life "Linden dollars"; PerfectMoney; WebMoney 'WM units'; and World of Warcraft gold."[10]

Decentralized currencies, by contrast, are created and maintained by an open community of interested participants using open source software. These participants run the software, or a compatible modification of the software, on Internet-connected computers that, together, form an open peer-to-peer network. Decentralized virtual currencies are also known as cryptocurrencies because all decentralized currencies, to date, have utilized theories and functions from the science of cryptography in order to guarantee both (A) that network participants cannot spend the currency held by other participants and (B) that the money supply grows at a predictable rate. Bitcoin, launched in 2009,[11] was the first cryptocurrency, and, as of 2015, it remains the largest by market capitalization.[12]

Even though cryptocurrency software is released and updated by an individual or group of individuals, *e.g.* Bitcoin's "Core Devs,"[13] these individuals cannot unilaterally change how the currency functions. To make any change to the currency, the updated software must be adopted by a majority of the peer-to-peer network. This network, composed as it will be of technologically sophisticated users, will audit the new code and likely reject any code that attempts to inject risk or fraud into the system. Network participants who choose to validate transactions on the network and update the public ledger are called miners.

With these distinctions in mind, it is clear that companies producing *centralized* currencies like Amazon Coin or (the now defunct) Liberty Reserve should be treated as administrators or issuers of virtual currency. Further, it is important that these companies be licensed due to the risks of consumer abuse and money laundering native to closed ledgers and consolidated power.

---

[9] *See* Amazon Inc., *Amazon Coins*, http://www.amazon.com/gp/feature.html?docId=1001166401; *see also* Wikipedia, *Amazon Coin*, http://en.wikipedia.org/wiki/Amazon_Coin.

[10] Financial Action Task Force, *Virtual Currencies: Key Definitions and Potential AML/CFT Risks*, (June 2014) *available at* http://www.fatf-gafi.org/media/fatf/documents/reports/virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf.

[11] *See* Satoshi Nakomoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, (May 2009) *available at* https://bitcoin.org/bitcoin.pdf.

[12] *See* Market capitalization of top cryptocurrencies *available at* http://coinmarketcap.com/.

[13] *See* List of Bitcoin Core Developers *available at* https://bitcoin.org/en/development.

It is not, however, clear whether any participants in a *decentralized* currency can be treated as administrators or issuers. To the extent that core developers and miners create (*i.e.* "administer" or "control") some of the software and provide some of the power that allows the network to function and generates new currency units (*i.e* "issuing"), these individuals may be interpreted as controlling, administering, or issuing virtual currency. However, to regulate these parties and require licensure is to regulate mining and software development as an activity, something the Superintendent has specifically sought to avoid.

To avoid this undesirable outcome, the department must qualify what types of currencies will be regulated at the level of control, administration, and issuance. The department should revise 200.2(q)(5) as follows:

> (5) controlling, administering, or issuing a ***centralized*** Virtual Currency.

And the Department should define Centralized virtual currency by borrowing from the FATF guidance:

> *Centralized Virtual Currencies* have a single administering authority—i.e. a third party that controls the system. An administrator issues the currency; establishes the rules for its use; maintains a central payment ledger; and has authority to redeem the currency (withdraw it from circulation).

The consumer protection implications of this distinction are not trivial and warrant heightened licensing requirements for centralized currencies over their decentralized counterparts. A business utilizing a centralized virtual currency can unilaterally decide to devalue consumer balances by issuing more currency, similar to how a normal financial service could choose to take on more debt. A cryptocurrency business is not at such liberty; it cannot unilaterally create more tokens because monetary supply is governed by an open, collaborative protocol of which they are only a small part.

A centralized virtual currency business can rearrange consumer balances, or refuse to honor a consumer credit, and it, ultimately, is the sole fiduciary of the currency's accounting records. A cryptocurrency business, even if it rearranges consumer balances once deposited, can only receive and dispense funds to a consumer by writing to an indelible and public accounting record, the public ledger or blockchain of the cryptocurrency. This ledger, unlike the closed, internal ledger of a centralized virtual currency business (or, for that matter, a traditional financial services business) can be publicly audited in real time to guarantee the solvency of the firm.

A centralized virtual currency business can operate using closed source software, meaning the underlying scarcity or safety of the currency cannot be easily audited by outside technologists. A cryptocurrency is open-source by default and the underlying fundamentals of that technology are scrutinized by a bevy of third-party validators.

In short, with this distinction—centralized versus decentralized—in mind, we can see that the consumer protection risks endemic to any particular virtual currency business can vary profoundly.

Regulations will affect how the virtual currency industry develops. Given that decentralized virtual currencies have some inbuilt consumer protections—owing to their open-source, decentralized, and transparent nature—it would be unfortunate if premature and indiscriminate regulatory action stifled the development of these technologies. To avoid this outcome, and to be certain that consumers are protected against technologies lacking in-built protections, the Department must ensure that it does not incidentally outlaw unlicensed mining or software development in decentralized currencies. Such incidental regulation can only be avoided by qualifying that 200.2(q)(5)—"controlling, administering, or issuing"—applies only to centralized currencies.

We recognize that the Department has added an explicit carve-out for software (though not for mining) at 200.2(q):

> The development and dissemination of software in and of itself does not constitute Virtual Currency Business Activity

While we applaud this addition and believe it should persist, it would not protect a Bitcoin developer or miner, as the Superintendent has promised, because these entities will generally do more than "software development and dissemination in and of itself." They will also connect to the network, process transactions, and maintain peer-to-peer nodes. The only way to avoid regulating these parties is by qualifying 200.2(q)(5) such that applies only to centralized currencies.

2. An On-ramp for Startups.

Virtual currency is exciting, in part, because it has brought new life and competition to markets for the provision of financial services. This vibrancy is not the result of careful scientific research or newly patented inventions developed by large technology firms. It is, instead, the result of many small start-up companies working with freely available software and an open network.[14]

Why Virtual Currency Startups Matter

Small firms are diverse, presenting consumers with many new options for financial transactions, and are also capable of scaling massively should their ideas gain widespread consumer traction. That diversity is contingent on low overhead costs inherent to open virtual currency networks, which allow a company to securely accept funds from a customer

[14] Angel.co, a valued trade publication within the technology investment community, lists some 619 companies that are now building Bitcoin related businesses. These companies, however, are small. Average valuation is estimated at $3.9 million. Angel.co, *Bitcoin Startups*, https://angel.co/bitcoin (last accessed Feb. 2015).

across the world in a matter of minutes for fractions of a penny on the dollar.[15] That network also enables scalability: transactions of many millions of dollars carry the same fees as transfers of pocket change and can be executed just as easily.[16] As technological limits on diversity and scalability are lifted, it is important that those limits are not merely reinstated by a costly regulatory structure that is insensitive to the small size or rapid growth of new and innovative players.

Discretion Alone Cannot Accommodate the Needs of Start-ups.

The revised Bitlicense rightly contemplates the need to exempt small and innovative virtual currency startups from the costly burdens of licensure. However, under the new BitLicense, those exemptions, called "conditional licenses," are granted at the "sole discretion" of the superintendent.[17]

Discretion can be an important tool for lessening the unduly harsh effects of a regulation, but it should not be the only tool. Discretion also generates regulatory uncertainty: a citizen never knows whether conduct she has freely engaged in before will suddenly become punishable simply because a government official changed her mind, or was replaced, or—in the worst case—was influenced by a competitor or someone who wished our hypothetical citizen harm.

A formal, rather than discretionary, carve-out for small startups is essential to preserve the freedom to innovate using these technologies, and it should be accomplished in a way that sets clear ex-ante standards and safe-harbors for budding entrepreneurs.

Drafting an On-Ramp for Startups

Accordingly, we strongly urge the Department to adopt an *on ramp for startups* in the virtual currency space. Companies that are very new and pose little threat to consumers could be conditionally exempted from licensure. For example, the Department could specify an exemption for firms dealing in less than $5 million in virtual currency annually. This exemption could be further conditioned on: (1) the business must register with federal money laundering authorities, and (2) must clearly disclose their conditional status to consumers. Firms with pending applications could also be offered a safe harbor, allowing them to operate while their license applications are pending; these transitional firms should similarly be registered with federal authorities, make clear disclosures, and if transacting greater than $5 million annually they can be required to post a standard bond pegged to the volume of business that they do.

---

[15] Popular hosted wallet provider Coinbase, for example, pays the Bitcoin network typically 0.0002 BTC for transactions of any size. They do not charge this fee to the customer choosing to bear these small costs internally. Coinbase, *Does Coinbase pay bitcoin miner fees?* (Dec 2014) *available at* https://support.coinbase.com/customer/portal/articles/815435-does-coinbase-pay-bitcoin-miner-fees-

[16] *Id.*

[17] 200.4(c)(3)(i)

We believe the $5 million per year transaction level is an appropriate threshold between companies that can pose serious, systemic risks to consumers (*e.g.* Mt. Gox), and those where risk level is tolerable given the benefits that unfettered start-up innovation could bring. However, the department could carefully calibrate this threshold as it sees fit. This threshold could change from time to time or be based on some other ex ante specification (*e.g.* a time-delimited safe-harbor for companies younger than two years), affording the superintendent some discretion to adjust regulatory policies in response to observed rates of fraud, consumer harm, or other extenuating circumstances. However, those adjustments should be explicit, apply generally across the industry, and be announced in advance so firms can plan their compliance strategies efficiently.

An On-ramp will Attract Virtual Currency Businesses to New York

Such simple, prospective rules allow an innovator to tailor her own behavior and optimize her business against known regulatory burdens. A New York virtual currency safe harbor would allow startups to quantify future regulatory liabilities by removing the inherent uncertainty of human discretion. Startups would be able to take this quantification of regulatory risk to their prospective investors, assuring them that the startup will be able to operate without encountering an existential threat, *i.e.* the unexpected costs from a failed attempt to seek conditional status.

Once the startup has grown because of the value and innovation it has created, clear language in New York's regulations would outline when and how it must become fully licensed. Treating innovators with such respect, by affording them the protections and predictability of clear ex-ante standards and safe-harbors will make New York a beacon in the otherwise pervasively uncertain landscape of state money transmission licensing.

A small team of innovators will at least know that in New York they need only meet a simple registration and disclosure requirement while they bootstrap, even if their operation in some 48 other jurisdictions may be clouded by the uncertain need to obtain a burdensome money transmission license. This team will know that their conditional status does not hinge on who currently holds a political office, or whether they've managed to negotiate effectively with that office, but rather on their own success as measured by transaction volume. The on-ramp, by simplifying the compliance calculus, would attract small and competitive new entrants and serve as a model for other states hoping to woo the jobs, tax-revenue, and prestige that these companies generate for their parent state.

3. New Product Pre-approval Will Hamper Innovation

The BitLicense requires that licensees seek pre-approval from the superintendent for any:

> [N]ew product, service, or activity, or to make a material change to an existing product, service, or activity, involving New York or New York Residents.

The product release and testing cycle for startups is different than for traditional banks. Startups will often pivot to new services or do trial tests (*i.e.* beta testing) of new services in order to probe markets for new opportunities. This experimentation is what allows for innovation despite uncertainty. The innovator does not know, *ex ante*, what will absolutely succeed, providing customers with the exact product they'd wanted all along. Instead, the innovator tries several products, often with a limited number of users or at small scale, in order to see what sticks. Innovators may even try two versions of a service simultaneously; this is referred to as A-B testing. Subtle differences between these two versions can reveal specific consumer preferences that can significantly improve the user experience. The agility to try several approaches is essential to innovation in the new and rapidly growing financial technology landscape. If New York licensed start-ups are forced to wait for pre-approval every time they seek to test a new service, these start-ups will likely miss opportunities seized by faster more agile competitors overseas.

We recognize that the department may need to reinvestigate salient features of its licensing requirements if new products gain traction and present a new risk profile. However, this can be accomplished by requiring notification of a new service rather than pre-approval. A licensee could be required to alert the Department of new or changed plans, yet be left free to execute these changes or bring new products to market during a grace period, while the Department determines if capital requirements need to be adjusted or if the new plan simply cannot be offered to New York customers. Switching from a *pre-approval* to a *notification and grace period* approach will allow for the benefits of permissionless innovation—new jobs and new consumer tools and choices—without hamstringing the department's ability to ultimately protect consumers.

Additionally, to be certain that only those changes and products that pose additional or new consumer risk trigger this process, the Department should define what precisely constitutes a "new product, service, or activity."

The Department has already defined "material change" to an existing product. An appropriate definition for new products, activities, or services could mirror that existing language as follows:

> A "new" product, service, or activity can be found when:
>
> > (1) a product or feature is materially different from that previously listed on the application for licensing by the superintendent;
> >
> > (2) the proposed product may raise a legal or regulatory issue about the permissibility of the product, service, or activity; or
> >
> > (3) the proposed product may raise safety and soundness or operational concerns.

Such clarification would prevent a uniformly inefficient outcome where businesses feel obliged to perpetually notify the Department of minor revisions to their software, and the Department is swamped with reams of annotated computer code.

4. The Department must Make Clear that a BitLicesnse Supplants the Need for Money Transmission Licensing

A virtual currency business should not need to acquire both a money transmission license and a virtual currency license. The Department's vision in creating a new technology-specific license is laudable. Existing money transmission rules are vague, offer little guidance to entrepreneurs, and do not intuitively lend themselves to cover this new technology. That leads to legal uncertainty, business inefficiency, and, ultimately, to poor and insecure consumer services.

That said, both kinds of licenses aim to accomplish the same thing. They are meant to ensure that companies are well-run, well-capitalized, and adequately serve consumers. Once a business has acquired a BitLicense, therefore, there is no apparent benefit from going through the expense and trouble of acquiring a second license. If a virtual currency company is adequately capitalized, vetted, and compliant with standards set case-by-case by the Department; what can be gained from a second set of examinations, invoked merely because the company holds fiat currency in addition to virtual currency?

The revised regulation remains unclear whether a BitLicense is required of virtual currency businesses *instead* of a money transmitter license or *in addition* to such a license. While the department's intention is no doubt the former, it should clarify this question to avoid any confusion. New York law requires that anyone engaged in "the business of receiving money for transmission or transmitting the same" must have a license issued by the superintendent. [18] Courts are increasingly coming to the conclusion that virtual currencies such as Bitcoin qualify as "money" under various statutory definitions.[19] Relatedly, any individual who "knowingly conducts, controls, manages, supervises, directs, or owns all or part" of a money services business operating without a money transmission license can be fined and imprisoned for up to five years under federal law.[20] The Department surely does not wish a BitLicensed company to remain technically in violation of federal law (should the requirement to have a *money transmission* license be interpreted strictly). The Department should therefore clarify that a BitLicense satisfies the statutory licensing requirement for money transmission.

[18] New York Banking Law § 641.
[19] See Securities and Exchange Commission v. Shavers, No. 4:13-CV-416 (E.D. Tex. Aug. 6, 2013) & United States vs. Ross William Ulbricht, No. 1:14-CR-00068 (S.D.N.Y. July 9, 2014) (each finding that bitcoins qualify as "money" for purposes for the statutes being enforced in each case).
[20] 18 U.S.C. §1960(a).

5. State Level AML Requirements Remain Duplicative and Go Beyond Federal Standards

We applaud the Department for qualifying the need to record recipient data for every transaction.[21] This qualification shows an understanding and accommodation of technological limitations as well as restraint in going beyond federal AML requirements. However, we continue to believe that the BitLicense's AML requirements go too far, imposing costs onto Bitcoin businesses that are not borne by any other money transmission business under state or federal law.

Specifically, the license has a state-level suspicious activity reporting (SARs) requirement,[22] the first of it's kind for state money transmission law, and a requirement that duplicates the efforts of FinCEN.[23] The state-level SARs requirement has no lower bound of application, potentially resulting in a flood of low-value reports that hemorrhage sensitive user-credentials and damage user privacy because of overly-cautious regulatory compliance. The license has a reporting requirement[24] that similarly doubles the efforts of FinCEN.[25] The Department has not explained why FinCEN and Federal regulators are failing at their remit and therefore need a second line of state-level reinforcements. Nowhere in New York or, for that matter, any state's money transmission licensing scheme are such AML requirements in evidence.

This, if not remedied, will make the BitLicense, and New York an unlikely home for international companies free to choose their base of operations and their regulator. Companies may choose to protect user privacy and avoid costly requirements by settling in, for example, the United Kingdom, which has recently shown a sensitive approach to virtual currency regulation.[26] To the extent necessary, these companies may screen the IP addresses of their customers and limit their services when dealing with New Yorkers so as to avoid embroiling themselves in a legal struggle with inherently large downside risks (time in prison) and little upside (a marginal number of additional customers from New York).

---

[21] Compare the initial proposed recordkeeping requirement at 200.12(a)(1): "(1) for each transaction, the amount, date, and precise time of the transaction, any payment instructions, the total amount of fees and charges received and paid to, by, or on behalf of the Licensee, and the names, account numbers, and physical addresses of the parties to the transaction" to the revised requirement: "(1) for each transaction, the amount, date, and precise time of the transaction, any payment instructions, the total amount of fees and charges received and paid to, by, or on behalf of the Licensee, and the names, account numbers, and physical addresses of (i) the party or parties to the transaction that are customers or account holders of the Licensee; and (ii) to the extent practicable, any other parties to the transaction."

[22] 200.15 (e)(3)

[23] FinCEN SARs requirements for MSBs

[24] 200.15(e)(2)

[25] FinCEN Reporting over 10,000 for MSBs

[26] *See* Jerry Brito, "The UK plan for Bitcoin is a step in the right direction" *Coin Center* (March 18, 2015) http://coincenter.org/2015/03/the-uk-plan-for-bitcoin-is-a-step-in-the-right-direction/.

The CSBS takes what we believe to be a reasonable position regarding AML and state virtual currency policy. It recommends:

> Required implementation and compliance with BSA/AML policies, including documentation of such policies. Required compliance with applicable ***federal BSA/AML laws*** and recognition of state examination and enforcement authority of BSA/AML laws[.]

This is standard is echoed in New York's own money transmission regulation:

> d. Compliance with applicable federal requirements shall constitute compliance with the provisions of this Part [Sec. 416.1 Anti-Money Laundering Programs].[27]

Moreover it is echoed by California, whose proposed licensing regime for virtual currency business makes no mention of AML requirements.[28]

If New York is serious about attracting virtual currency business, it must not place a greater burden on these firms than it places on traditional money transmitters. It must not place a greater burden on firms than would California, or the United Kingdom. If New York sets this onerous example, other states across the country may follow suit or, worse, may create some unique concoction with still more incongruent standards. Calibrated compliance with each of these disparate AML regimes (not even mentioning global jurisdictions) would surely sap an innovator of her capacity, capital, and will to build anything of use, a great loss to users and economies. Accordingly, we strongly urge the Department to adjust its AML requirements to match Federal standards, and mirror the language of its money transmission regulations, specifying that "compliance with applicable federal requirements shall constitute compliance with the provisions of this part."

If, however, the Department believes these requirements to be *absolutely necessary*. We strongly urge the Department to at least place a lower bound on its SARs requirement, so that the privacy of New York residents is not unduly threatened by over-zealous reporting of their transaction histories. FinCEN has carefully calibrated its SARs requirement and the Department should follow suit: SARs should be required only when a transaction exceeds $2,000 and the institution suspects or has reason to suspect that the transaction (a) involves funds derived from illegal activity or (b) is designed to evade the requirements under the Bank Secrecy Act, or (c) serves no apparent or lawful purpose and the reporting business knows of no reasonable explanation for the transaction after examining all available facts.[29]

---

[27] http://www.dfs.ny.gov/legal/regulations/adoptions/banking/ar416tx.htm

[28] An act to add Division 11 (commencing with Section 26000) to the Financial Code, relating to virtual currency, A.B. 1326, California Legislature 2014-2015 Regular Session (February 27, 2015) *available at* http://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201520160AB1326

[29] *See* 31 C.F.R. § 1022.320.

6. Protection Is Still Needed for Lawful Obfuscation

Many virtual currencies, including Bitcoin, publically reveal a great deal of potentially private transaction information. Every transfer to and from every public address since the invention of Bitcoin is recorded on a public ledger known as a block chain.[30] Although pseudonymous, this address information can potentially be traced back to the individual, revealing the individual's financial and transaction history.[31]

The financial privacy repercussions of this open-by-default system are even greater when one considers that a potentially popular use for digital currencies is to make micropayments.[32] Traditional payment methods generally require large, fixed minimum processing fees. This makes their use for very small payments uneconomical.[33] These very low value purchases could, nonetheless, be highly useful for the provision of certain goods and services. For example, an online newspaper may wish to charge 10 cents to grant a reader one-off permission to read an article.[34] Similarly, a telecommunications provider may wish to charge half a cent to connect to a Wi-Fi router for a matter of seconds or minutes as the customer moves into and out of the router's range. Cryptocurrency micropayments could allow new markets to develop that have previously been made impossible by the transaction costs of traditional payment systems. This, in turn, could revolutionize entire sectors of the economy, especially media, which has heretofore been overwhelmingly dependent on advertising, and collection of information about users' likely interests that makes modern advertising effective and profitable for media.

Micropayments, however, could create an extremely detailed picture of a user's activities throughout the day. They could indicate, with specificity, every article the individual has read and every Wi-Fi router the individual has passed while going through their daily routine. Given the depth of this account, it is important that Virtual Currency users be permitted to obfuscate transactions so that they are not—as would be the Virtual Currency

---

[30] Copies of the block chain are stored on the hardware of all miner clients and many wallet nodes in the Bitcoin network. The blockchain can be explored using free tools on websites such as https://blockchain.info/.

[31] *See* Elli Androulaki, et al. "Evaluating User Privacy in Bitcoin," 7859 *Financial Cryptography and Data Security Lecture Notes in Computer Science* 34 (2013) (Finding that "behavior based clustering analysis" and the monitoring of publicly available information on the block chain can allow for de-anonymization after wrongdoing is detected by observing transactions.).

[32] *See* Marc Andreessen, "Why Bitcoin Matters," *NY Times* (Jan. 21, 2014), http://dealbook.nytimes.com/2014/01/21/why-bitcoin-matters/.

[33] For example, on the Visa payments network, interchange fees for card-not-present transactions vary from 15 to 25 cents plus a percentage of the total payment. *See* Visa, *Visa U.S.A. Interchange Reimbursement Fees* (Apr. 2014), http://usa.visa.com/download/merchants/Visa-Interchange-Reimbursement-Fees-April-2014.pdf. This makes Visa uneconomical for purchases under or near the 15 to 25 cent range. (If a good or service is worth only, say, fifty cents, increasing its total price by half, to seventy-five cents, may effectively make it uneconomical.)

[34] *See* Walter Isaacson, "How Bitcoin Could Save Journalism and the Arts," *Time* (Oct. 7, 2014), https://time.com/3476313/can-bitcoin-save-journalism/.

default—publicly associated with the same user address with each transaction. The BitLicense should instead permit Virtual Currency businesses to scramble transaction records as they appear on the public blockchain, so long as they can continue to meet their recordkeeping and reporting obligations. In other words, users should have the option of choosing services that hide their detailed payment history from public view, as long as law enforcement can still access that data from licensed intermediaries.

Section 200.15(f) presently reads:

> "No Licensee shall engage in, facilitate, or knowingly allow the transfer or transmission of Virtual Currency when such action will obfuscate the identity of an individual customer or counterparty. Nothing in this Section, however, shall be construed to require a Licensee to make available to the general public the fact or nature of the movement of Virtual Currency by individual customers or counterparties."

This passage should include a second savings clause to ensure that Virtual Currency businesses remain free to take steps to prevent the full records of their customer's transactions from being publically visible:

> "Nor shall anything in this Section be construed to prohibit the good faith obfuscation of customer or counterparty identification to maintain consumer privacy as against the general public while complying with the customer identification program described in Section (g)."

The Department no doubt values the privacy of virtual currency users and wishes licensed firms to protect that privacy. It must therefore clearly insulate these firms from legal liability as described above.

Conclusion

To be a leader in the future of financial technology, the Department must carefully forge a path toward consumer protection and avoid the pitfalls of inartful, unnecessarily costly regulation. As described throughout this comment, that path has several essential steps (1) that only those with unilateral control be subject to a license requirement, (2) that innovative and small startups be protected with a non-discretionary on-ramp, (3) that changes of business require notification rather than pre-approval, (4) that BitLicensed firms need not seek a duplicative money transmitter license, (5) that AML requirements match and don't exceed federal standards, and (6) that firms may protect user privacy by lawfully obfuscating transactions from the public. The Department will be the first to travel this craggy and dimly-lit terrain, but it will not be the last. May it discover a path worth following.