



October 21, 2014

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

**Re: DATA's Public Comments to NYDFS Proposed Regulations: Title 23,
Chapter I, Part 200: Virtual Currencies**

Dear Mr. Syracuse:

This letter is submitted to the New York State Department of Financial Services (“NYDFS” or the “Department”) on behalf of Digital Asset Transfer Authority (“DATA”) in response to the notice of proposed Virtual Currency Regulations published on July 17, 2014 (the “Proposed Rule”). NYDFS has an important public policy mandate to protect consumers, and adapting existing legal regimes to new technologies is not an easy task, particularly in the context of lengthy rulemaking and comment process, and rapid evolution of new technologies. We recognize this inherent challenge and NYDFS’ leadership in offering the first attempt to encompass digital asset firms in its regulatory framework, “to strike an appropriate balance that helps protect consumers . . . without stifling innovation” which has already sparked meaningful debate on these critical issues.¹ We are therefore grateful for this opportunity to share the knowledge base and subject matter expertise from DATA members on this important piece of proposed regulation, which will not only shape the future of digital assets in the state of New York, but serve as a reference point for other jurisdictions in the US and abroad. New York is one of the financial hubs of the world in an increasingly globalized economy. As globally interoperable technologies such as the Internet, Skype, and Bitcoin continue to emerge, we hope that New York’s rulemaking and governance processes can continue to evolve at pace with the technologies and legal frameworks around the world, so that New York can remain a leader in our global financial network in the 21st century. To that end, we have reached out to our members for their initial feedback, comments and concerns regarding the Proposed Regulations, which are provided below.

¹ New York State Department of Financial Services, “NY DFS Releases Proposed BitLicense Regulatory Framework for Virtual Currency Firms” (Press Release, July 17, 2014), <http://www.dfs.ny.gov/about/press2014/pr1407171.html>.



I. Background of DATA

DATA is a global non-profit trade association established in July 2013 focused on digital assets, including distributed ledger technologies such as Bitcoin.² DATA's overarching goal is to act as a conduit and feedback mechanism between the digital asset community, policymakers and subject matter experts, and to inspire confidence in such products by spearheading the development of best practices across AML, data security, consumer protection and privacy, and to evolve in compliance with applicable laws and regulation governing digital currencies including decentralized ledger technologies such as the Bitcoin protocol (referred to collectively herein as "digital assets"). Our members represent a broad range of Bitcoin and other digital asset businesses including currencies, exchanges, administrators, and payment platforms, as well as service providers such as established law firms that are actively engaged in the digital asset space.³

II. Active Industry Steps Towards Self-Regulation

The industry has organically developed best practices over the last year, including prophylactic AML programs even for businesses that may not require it, real-time pattern monitoring and link analysis, clear consumer disclosures, proof-of-reserves, cold storage, multi-signature wallets, peer-reviewed altcoins, sophisticated onboarding metrics, blockchain SARs, complex disaster recovery and incident response plans, restricted data access, transparent balance sheets, and user-enabled audits, among others. In stark contrast to the "wild west" misconception of the Bitcoin industry, in the weeks following the Mt. Gox collapse, to assure consumers of the safety of their funds, leading Bitcoin exchanges and wallet providers spearheaded independent security audits that enabled the consumer to independently verify their balance on the

² More information available at www.dataauthority.org.

³ The name of our organization originated from two deliberate semantic choices: (1) we chose "digital" instead of the term "virtual" used in FinCEN's March 2013 Guidance because the latter implies that these technologies, and the value creation of these networks are limited to virtual gaming environments"; and (2) we fundamentally recognized that technologies such as Bitcoin challenge the traditional labels for existing asset classes, and that decentralized technologies and networks - along which any asset class can be tethered to travel - represent newly emerging asset classes. As an umbrella organization for these technologies, we chose the terms "digital asset" to underscore that Bitcoin and other emerging technologies can and do function like asset classes other than currency. They may require a retooling of public policy goals for each asset class, and corresponding rules and regulations to achieve those goals in a new technology context. One can imagine the absurdity of applying postal mail regulations to email technologies, or the application of the "duck" test to a technology like Bitcoin that can, indeed, walk, talk and quack like many different asset classes.



blockchain on their personal computer or mobile device.⁴ In the traditional financial world, this would be the equivalent of banks opening their balance sheet to the public within weeks of the 2008 financial crisis and enabling customers to independently check that their funds are, in fact, held by their depository bank. More over, while we have much to learn from the banking world about physical security, auditing, and accounting procedures, the traditional banks have much to gain from the technologists and innovators of the digital asset world that can enable them to leverage these technologies to vastly improve their own systems for consumers and free capital flows.⁵ The digital asset industry may be young and emerging, but these entities and individuals have demonstrated more proactive steps than any other financial services industry to date, and have been and continue to be committed to engagement and dialogue with all stakeholders to meet public policy goals and offer more resilient services.

III. Lessons of the Internet and Open Platforms: Centralized to Decentralized Systems

As an increasingly globalized community, society is undergoing a paradigm shift in models of business, governance, and culture. We are fortunate to have the benefit of hard won lessons from the early days of the Internet, when emerging communication and information technologies challenged existing business models and legal structures. Information became immediately accessible and digitally reproduced, communication became social, user-generated content became instantaneous, forcing business models to adapt and companies to monetize content in different way. We even had to reconceptualize speech on the Internet and build new frameworks for liability for online service providers and third party users on technology platforms.

We also learned how open systems flourished where closed ones failed. We learned how permission-less innovation allowed entrepreneurs to test new business models on a global scale. With the Internet, we learned that an experimental open source platform, with no central authority, corporate controls or government sponsorship, one that was deeply flawed in its first iteration and lacking in security, mobility, trust, massive content distribution or privacy, could create new economies and enhanced economic value. Finally, we learned that a grand experiment like the Internet could evolve and improve over time from a community of developers, who added security (SSL, HTTPS), mobility (cloud), and other improvements over time.

⁴ See, e.g., Nermin Hajdarbegovic, "Kraken Bitcoin Exchange Passes 'Proof of Reserves' Cryptographic Audit", March 24, 2014, available at <http://www.coindesk.com/krakens-audit-proves-holds-100-bitcoins-reserve/>; see also <https://www.kraken.com/security/audit> and <https://www.cryptocoinsnews.com/okcoin-passes-bitcoin-proof-of-reserves-audit/>.

⁵ See CEWG BitLicense Comment Letter.



Today we are again at an inflection point in which the decentralized nature of the Internet is shifting paradigms of payments and asset transfers. Today's financial system operates from a centralized model, with central banks and clearing houses.⁶ While payments have become digitized and banks have come online, "when payment systems were first computerised, the underlying processes were not significantly changed...Distributed ledger technology represents a fundamental change in how payment systems could work."⁷ The Bank of England recently stated in its Q3 2014 Report on Digital Currencies:

[T]he key innovation of digital currencies is the 'distributed ledger' which allows a payment system to operate in an entirely decentralised way, without intermediaries such as banks. This innovation draws on advances from a range of disciplines including cryptography (secure communication), game theory (strategic decision-making) and peer-to-peer networking (networks of connections formed without central co-ordination).⁸

Now, the impact on the Internet on the traditional financial services networks challenges us to finally address the lack of privacy and trust in the original design of the Internet. Today's privacy and compliance practices have their origins in the 1970s, before the Internet, mobile phones, the Internet of Things, machine learning, Big Data, and Bitcoin. It is a very different world now. The time has ripened for a fundamental reconceptualization and reimplementation of identity, privacy, and related financial regulatory processes. And how we address expanding inequality driven by financial and technological access or its lack thereof, will influence not just our economy, but evolution as a global interdependent community.⁹

⁶ As Greg Brockman, CTO of Stripe, recently commented: "[t]raditional payment systems look a lot like computer networks before the Internet", July 21, 2014, available at <https://stripe.com/blog/bitcoin-the-stripe-perspective>.

⁷ Robleh Ali, John Barrdear, Roger Clews, James Southgate, Bank of England Quarterly Bulletin 2014 Q3, p.1, "Innovations in payment technologies and the emergence of digital currencies," available at www.bankofengland.co.uk/publications/Documents/quarterlybulletin/2014/qb14q3digitalcurrenciesbitcoin1.pdf ("Bank of England 2014 Q3 Report").

⁸ *Id.* at 1.

⁹ Terry Waghorn, March 11, 2013 Interview with Hazel Henderson, *Forbes Magazine*, available at <http://www.forbes.com/sites/terrywaghorn/2013/03/11/hazel-henderson-there-is-21st-century-abundance-hiding-in-19th-century-scarcity-politics/>. ("***The deepest shift is from 19th century scarcity economics' 'shortage of money' paradigm to Information Age abundance. Unlike material goods, information is not scarce.*** If you give me information, I am enriched along with you! This is the basis of the sharing, networking, open-source, peer-to-peer economies now emerging in crowd-funding, such as by MOSAIC, community currencies, credit unions and cooperatives (which employ more people worldwide than all global corporations combined). . . As communities worldwide create their own money like some 200 small



IV. Specific Comments

Below are some key areas of concern we have identified for NYDFS to reconsider for its second iteration of the Proposed Rule. We have also provided a list of specific concerns to the current proposal.

1. The Scope of Regulated Activities Is Overbroad

The blockchain – the distributed public ledger – provides manifold applications and uses beyond that of money or payments, including proof of existence, ownership, accounting, communication, transparent governance, among others. As written, the definition of “Virtual Currency Business Activity” is too broad. We agree that entities that act as intermediaries or depository institutions should be licensed and regulated. However, the current definition would apply licensing requirements to open source server software, desktop and mobile wallet software, mining pool software providers, online wallet software, and other open source digital currency and distributed ledger projects. Many who wish to build products and services based on these new Internet protocols that do not pose similar risks would be unfairly caught in this broad and burdensome net. Software companies should not be subject to government oversight in this manner, nor should uses of blockchain technologies that do not involve financial activity. The definition should be revised to specifically exclude individuals that seek to store, access and transmit value through their personal digital currency wallets.

Because money transmitter laws, which are now being adapted to these new technologies, are essentially “safety and soundness” statutes designed to ensure that consumer funds are protected from loss,¹⁰ we believe that the appropriate scope of licensed activity should only extend to those entities engaged in activities that involve true custodianship of funds and corresponding risk of loss to the consumer. Sections 200 (l)(m) and (n) need to be revised to eliminate from licensure requirements those that only write code, offer security or other non-custodial services, and process payments. As written, the Proposed Rule covers anyone that receives or transmits virtual currency – in essence, anyone that uses digital assets. The application and oversight requirements should only apply to those that have the unilateral ability to transfer or lose customer funds.

We also note that the Proposed Rule seeks to regulate entities and activity that fall within a broad definition of “virtual currency business activity” “involving New York

cities in Brazil, *people realize that money isn’t scarce but a form of information. Money is not wealth but a useful unit of account tracking our human transactions.* If not abused or inflated by today’s banks, money can be a store of value.”)

¹⁰ See Uniform Money Services Act, prefatory note, 7A U.L.A. 163–64.



or a New York resident.” We are encouraged that you recently clarified in a speech that your jurisdiction was only intended to reach “New Yorkers doing things in New York”, and request that the statute reflect the same.

Furthermore, because the regulated activity is quite broad, it necessitates expansion and clarification of exceptions. As written, the proposed regulations do not include traditional exemptions for money transmitters, banks and or agents of entities with requisite licenses. The customer and merchant exception also needs to be expanded and clarified to provide certainty as to what constitutes engaging in “virtual currency business activity” including “buying and selling as a customer business” distinguished from those that merely “utilize virtual currency solely for the purchase or sale of goods or services.”

In general, the definitions are unnecessarily broad and subject the nascent digital currency industry to regulations far harsher than the existing money transmission framework without clear risk/benefit analysis. While regulatory certainty has its benefits, without further clarification, the Proposed Rule – including the broad scope of potentially captured activities, drafting ambiguities, and failure to exempt certain activities on a risk basis in context of new technologies - cast too wide a net and would lead to less certainty and innovation.

2. New AML Requirements Pose Serious Privacy Issues and Untenable Data Collection Requirements.

DATA believes that the expansion of AML oversight at the state level is unnecessary and would provide more inefficiencies, with parallel tracks of regulatory and compliance costs, for little gain.¹¹ The federal system in the United States provides adequate federal oversight and is in line with requirements in other foreign jurisdictions, including Canada and Singapore, which require registration, recordkeeping and reporting. The Financial Crimes Enforcement Network (FinCEN) issued guidance on March 18, 2013 that clarified which digital currency businesses are subject to money services businesses regulations under the Bank Secrecy Act, including full KYC, transaction monitoring, recordkeeping and reporting. There is no need for a parallel track of AML, particularly where traditional methods have created demonstrated privacy and security risks while driving up enormous costs with little efficacy.

¹¹ In its 2014 Global AML Survey, KPMG found that the cost of compliance rose at an average rate of 53% year over year of its survey from 2011-present, that over 88% respondents said their Boards of Directors actively discussed AML, but found that the improvements in transaction monitoring and KYC only rose very incrementally. See KPMG 2014 Global AML Survey, p. 8, 14, 24, available at <http://www.kpmg.com/Global/en/IssuesAndInsights/ArticlesPublications/global-anti-money-laundering-survey/Documents/global-anti-money-laundering-survey-v5.pdf>.



NYDFS should eliminate the requirement to collect full identity information for both senders and recipients. As the Proposed Rule stands, companies who obtain a BitLicense must collect personal data on both parties to any transaction, including full name and physical address, and keep that data for ten years, even for de minimus transactions. No public policy justifies the collection of PII for every de minimus transaction – there is no net gain, only additional burden to the licensee and privacy risk to the consumer. At a minimum, this section needs to be revised to eliminate the requirement for PII collection of non-customer of the licensee (as it is not feasible in decentralized, open networks) and indicate a minimum transaction threshold for identity verification (e.g., base policymaking on risk/benefit calculation). To do otherwise would prevent companies from establishing presence in New York or servicing its consumers.¹² Section 200.15 is also not risk-based and would eliminate visibility into these transactions by driving users to unlicensed companies. And as the recent massive data breaches at Target, Home Depot, Kmart and JP Morgan show,¹³ the continued practice in the e-commerce and banking world of personal data collection to process transactions, a practice that originated in a brick-and-mortar world, present serious dangers to privacy and control of our identities. By proposing massive expansion of data collection for all transactions and requiring PII to be held for ten years, NYDFS exacerbates the privacy and self-sovereignty problem without any corresponding benefit in trust, identity verification, or risk reduction.

DATA believes the focus should be on proportionate access to identity and transaction information to achieve those specific public policy goals (purpose), rather than an unsubstantiated right to the information itself (means). In a world where “closed shops” of private institutions have morphed into a transparent public ledger visible on the Internet in real-time to regulators and law enforcement, these stakeholders have unprecedented visibility into the transaction networks. It may be unnecessary to continue to commandeer private institutions to collect ever more personally identifiable information for analysis after the fact, with a personally identifiable data trail for every transaction for ten years regardless of amount. The requirement that every transaction include name and physical address for all parties would remove the possibility of having any cash-like interactions in the digital economy. Moreover, the essential transparency of the public ledger, which renders detailed financial information that can easily be tied to individuals, underscores the necessity to develop new tools that

¹² “Xapo Will Have No Choice But To Leave New York”, available at <https://xapo.com/post/xapo-will-have-no-choice-but-to-block-new-york/>; see also https://www.circle.com/en_US.UTF-8/2014/08/13/thoughts-new-york-bitlicense-proposal (“Circle will have no choice but to block New York customers from accessing our services”).

¹³ Jake Swearingen, “Why the JP Morgan Data Breach Is Like No Other”, *The Atlantic*, October 3, 2014, available at <http://www.theatlantic.com/business/archive/2014/10/why-the-jp-morgan-data-breach-is-like-no-other/381098/>.



enable consumer privacy to the public writ large.

3. Government Given High Level of Discretion Over Businesses

DATA believes that the permission-based aspects of the Proposed Rule will heavily stifle innovation and are infeasible business practices for technology companies. The Internet owes much of its ubiquity and value creation to its open source, permissionless nature. The current proposal creates an explicit, permission-based regulatory framework that no business could submit to, even if willing, as it would cripple its ability to operate. For example, the Proposed Rule requires advance submission and approval of new features and product changes and oversight over key business decisions, all of which are anathema to digital currency businesses. These are startups that must continuously iterate software development and business models, particularly in this rapidly evolving ecosystem and consumer needs. The four-month review period for NYDFS approval of any change in control of 10% would cripple the funding and development process of these companies, and far exceeds the 25% analogous threshold for NY money transmitters without a principled basis. The proposed regulations also require prior written approval from New York regarding mergers and acquisitions, an extraordinary requirement not applied to money transmitters.

There are other areas of concern regarding the scope of NYDFS oversight, including the discretionary bond and capital requirements, and rights of access, inspection and examination. For example, the Proposed Rule sets forth capital requirements “the superintendent determines is sufficient”, without providing a reliable methodology to provide clear guidelines for and expectations of applicants.¹⁴ DATA believes that the regulations must provide for a robust appeals process to ensure due process and foster confidence, transparency and trust regarding NYDFS’ policies and decisions.

4. Need For a Principled, Risk-Based Framework

DATA believes that regulations should be transparent and proportionate, based on assessment of the risk and weighed against the benefit of these technologies. A one-size-fits-all regulatory scheme that fails to differentiate between the unique risks of each potentially regulated activity will stifle innovation without materially advancing the statutory goals. However, that does not necessarily require the creation of a new regulatory framework for a nascent industry that has yet to bring to market the next generation of these distributed ledger protocols. NYDFS can achieve its goals by adapting its existing state money transmission statutes to address digital assets on a

¹⁴ Cf. EU Payments Services Directive.



principled- and risk-basis that can withstand the tests of time and rapid technological advances. Two statutorily vague frameworks will not result in the regulatory certainty NYDFS and market participants seek, but rather, the opposite. We are concerned that, as a whole, these regulations appear to impose far greater burdens on digital currency firms than their money transmitter or financial institution counterparts (for some business models), despite the fact that these regulations were meant to tailor the statutory goals of money transmission rules in this new technology context to better enable innovation. Because the industry is in its infancy and technologies are rapidly evolving, a risk-based framework that enables a level-playing field and evolves with technological advances would allow NYDFS to fulfill its challenging dual role of regulating consumer risk while fostering an environment for innovation.

For example, these regulations purport to cover a much vaster range of activities than money transmission, require massive data collection, mandate separate state-level AML program, increase supervisory discretion, access and business oversight, and impose additional requirements. Requiring more evidence of “safety and soundness” of entities that pose less risk of consumer loss is questionable. Creation of a separate state-level AML framework for technologies companies operating with a public ledger that enables real-time pattern monitoring but not requiring such a program for proprietary “closed shop” banks and financial institutions, also seems to indicate a risk-based approach. There is also an open question as to whether the BitLicense is necessary where other states such as Texas have successfully adapted existing money transmitter statutes to address additional risks posed by digital currencies.

In crafting these new regulations, we urge NYDFS to focus on a principles-based framework that mandates rules in the context of the actual risks rather than a mere expansion of the old frameworks. This principles- and risk-based approach clarifies the scope of regulation while appropriately recasting state money transmitter laws to accommodate technological advances and a rapidly evolving ecosystem.¹⁵ This approach will also allow NYDFS regulations to evolve at pace with the digital currency ecosystem, providing it with clear principles that can guide today’s industry as well as the next iteration of market developments.

DATA believes there is an immediate need to create a tiered, risk-based onramp to an

¹⁵ The need to ascertain the scope and applicability of existing laws and regulations in light of new and emerging technologies is nothing new. See, e.g., *Am. Libraries Ass’n v. Pataki*, 969 F. Supp. 160, 161–82 (S.D.N.Y. 1997) (noting that (1) judges and legislators are “faced with adapting existing legal standards to the novel environment of cyberspace,” (2) the “Internet . . . requires a cohesive national scheme of regulation so that users are reasonably able to determine their obligations,” and (3) the “[r]egulation on a local [l]evel . . . will leave users lost in a welter of inconsistent laws, imposed by different states with different priorities”).



otherwise high barrier licensing regime, including a safe harbor provision that: (1) takes into account the rapidly evolving technologies and business models; and (2) ensures that regulatory requirements correspond to actual risk to the consumer and are balanced against the net public benefit of the technology. At a minimum, this safe harbor should allow small startups to operate in risk-bound settings, with minimum thresholds, and clear guidance on correspondingly light safety and soundness requirements, with at least six months to apply for a license once thresholds are crossed. The safe harbor approach has worked well in other technology contexts. Bitcoin and other digital assets are open source Internet protocols with potential to allow innovators to immediately develop and test beneficial products and services on a global scale in ways we have yet to imagine. Any geographically localized regulatory framework should, in addition to addressing risk, endeavor to leverage these consumer benefits and culture of innovation with minimal friction.

5. Leveraging Technological Advances for Effective Governance and Innovative Products - Redistribution of Public Policy Balance

Digital assets like Bitcoin present very real opportunities for enhanced governance and oversight because every transaction on the Bitcoin network is recorded on a distributed public ledger in real-time. Thus, technological innovations present as many opportunities as it does challenges to existing structures, by enabling stakeholders to leverage new technologies for more effective processes and outcomes. The perceived binary between effective oversight and privacy is false. Both are possible in the 21st century world. The very family of encryption technologies that make Bitcoin possible also make it possible to protect privacy and provide more tailored and effective governance. The key takeaway for financial regulators grappling with the difficult challenge of swiftly reimagining and retooling old regulatory means to a decentralized world, is that identity technologies as well as computational resources have evolved to the point where it is now feasible to authenticate identities without revealing identities. Technologies can now enable computations to verify personal information without necessarily disclosing the person's identity to third parties without probable cause. Regulators can thereby acquire the minimum requisite data to perform their oversight obligations without compromising individual privacy. These new methods of proportionate oversight and privacy-enabling identity verification are possible because there are now secure, protected processes and computations that enable individuals to protect their personal information and identities while also allowing selective interventions that assure highly effective KYC and AML compliance.

Other careful review of the public policy goals of regulations as applied to these emerging technologies will undoubtedly yield further retooling and reimplementations for important policy purposes. Technological tools may fundamentally alter the public



policy balance in other areas of regulation for these emerging asset classes. For example, the advent of multi-signature software in which the end user retains the ability to send funds, or private key custodianship methods, may render the wallet service provider a non-custodian, and the end user a non-accountholder. Further, the ability for firms to provide real-time cryptographic proof of reserves or continuous real-time accounting for the end user may move the means to protect against insolvency from burdensome and unwieldy government oversight to something consumers can oversee directly themselves.

Thus, while decentralized systems, like any other system, can be exploited to abet some crime, it prevents other crimes and circumscribes more effective governance in new ways. In another example, decentralization provides new opportunities for resiliency and redundancy in the financial network. The Bank of England notes in its 2014 Q3 report that Bitcoin's decentralized model is more resilient to systemic operational risk than centralized models because there are as many redundant backups as there are contributors to a decentralized network whereas the centralized model provides central points of failure.¹⁶

Policymaking for decentralized technologies from the Internet to Bitcoin require more participants, with risk-based not inherited barriers to entry, and scalable design requirements that strike the correct public policy balance. In order to strike that balance, costs and benefits must be quantified, not merely long-cherished narratives of historical costs and benefits. These calculations are impossible in a vacuum, with unsubstantiated claims of systemic risks, consumer risks, and public benefits. The key challenge is to design policy frameworks, based on clear principles, which are resilient enough to allow innovators to test the public benefits/risk of their technologies with minimal consumer and systemic risks, and to provide feedback mechanisms – technical and human – by which the public policy balance is reiteratively calibrated.

V. Comments for Specific Sections

Section 200.2(l) – Transmission

We request clarification regarding the term “transmission” in Section 200.2(l), which appears to include only activities conducted through “third parties” including transfers through processor, card and bank networks that fund digital currency wallets. Please clarify that individual wallet holders, software providers, and third party processors, card networks and banks were not intended to be included in the definition of “transmissions.”

¹⁶ Bank of England 2014 Q3 Report at 10.



Section 200.2 (m) – Virtual Currency

We are concerned that all digital assets, including digital tokens ascribed for ownership and transfer of other assets, including physical, as well as proof of existence on the public ledger, have not been expressly excluded from the definition of “virtual currency.” Because blockchain technologies enable manifold non-financial uses, special care should be taken to limit the definition to true currency-like products. It is helpful that the definition of virtual currency specifically excludes gaming units or points issued for reward programs, but others have raised questions about whether this definition might also encompass prepaid or stored value programs denominated in dollars or other fiat currencies. There is also a lack of distinction between open and closed loop networks and the failure to address the eventual fungibility of “closed” loop currencies within open or secondary systems. The use of digital tokens to facilitate other asset transfers, communications, and non-financial uses of distributed ledgers, should not be regulated under the Proposed Rule.

Section 200.2 (n) – Virtual Currency Business Activity

This one section of the Proposed Regulations received an overwhelming number of comments and concerns. That is because the NYDFS’s definition of “Virtual Currency Business Activity” is extremely broad, essentially including any digital assets-related business other than acceptance by merchants or use by consumers. Activities such as software development, mining or personal sale or transfer of digital assets might also be covered.

Our members believe that the NYDFS should consider either narrowing the definition or adding additional exemptions for those businesses which do not pose undue risks and do not provide hosted storage or exchange services. When the NYDFS includes under its purview many services that never actually access user funds, we believe that may be overreaching. These include in this category wallets like Blockchain.com, tipping apps like Changetip, and mixing services like CoinJoin. The inclusion of non-hosted wallets is especially troubling as it essentially outlaws the personal possession of bitcoins for these users unless such users obtain licenses. This is a result that we do not believe was intended.

The list of activities in 200.2(n) “securing, storing, holding, or maintaining custody or control of fiat currency on behalf of others” is an exhaustive and impermissibly overbroad list for purposes of licensing. Financial regulations that relate to depository institutions should not be blanket applied to technology providers that do not have true custodianship of customer funds, even if some of their services allow them to “secure”



or “hold” virtual currency on behalf of consumers as currently defined in Section 200.2(n)(2). This section needs to be revised and restricted to those businesses that have the unilateral ability to transfer funds.

Section 200.2 (n) (3)

The definition of what it means to buy and sell digital assets “as a customer business” requires clarification. As written, it can encompass nearly any activity that involves digital assets. Again, this definition casts too wide a net and frustrates the purpose of regulatory certainty.

Section 200.2 (n) (5)

Under the Proposed Rule, any party “controlling, administering or issuing a virtual currency” will require licensing. Not only does this subsection potentially cover an individual’s use of his or her private key to “control” one’s wallet, it also covers development of digital currency protocols. This provision would have outlawed Satoshi Nakamoto’s original bitcoin invention, and it certainly seems to ban any new alt-currencies and tokens that might be created in the future. Not only is the prohibition on writing software unconstitutional, the detrimental effect this would have on innovation in New York and across the US cannot be understated.

Section 200.3(b) - Agents

This section prohibits licensed digital assets businesses from conducting any business activity through unlicensed agents. This is markedly different from the rules that apply to licensed money transmitters. Today a licensed money transmitter that distributes money orders or prepaid cards can do so through unlicensed agents, with the licensed entity retaining full responsibility for their agents’ performance. It seems unfair that this basic structure would not be permitted for licensed digital assets businesses. We have not heard a risk basis for why licensed digital assets businesses should be subject to greater restrictions, like these, than those that apply to licensed money transmitters. As a rule, we believe that rules should apply consistently to promote free competition in the marketplace unless there is a principled or risk basis to do otherwise.

Section 200.3(c) – Exemption

This section, which outlines exclusions from licensing, also raised questions from our members. The exception for institutions “chartered under the New York Banking Law



to conduct exchange services” was puzzling. We seek clarification as to whether this intended to include banks or only non-bank licensed currency exchanges. We believe exclusions for broker-dealers, government entities, and other typical exclusions are warranted to level the playing field among various financial services providers.

Section 200.4 - Application

The application process for a license under the proposed regulations is similar to many other licensing application processes. But in some ways it is significantly more burdensome. For example, of course, fingerprints and detailed background information should be required for all principal officers and principal shareholders (owning 10 percent or more). But requiring fingerprinting and photographs of *all employees* is unusual and certainly (when fees are also applied) financially burdensome. In addition, the requirement to provide all written policies and procedures in connection with an application should be narrowed for relevancy and track obligations imposed on other financial intermediaries. Again, there seems to be little basis to arbitrarily subject digital currency firms to such extraordinary requirements that are not imposed on licensed money transmitters.

200.6 – Actions of the Superintendent

The Proposed Rule grants considerable discretion to the Superintendent’s office with respect to licensing, bonding and capital requirements with no indication of guidelines or guidance. NYDFS goals in providing regulatory certainty for market participants would be frustrated because of the opacity of discretionary decisions. Clearer capital requirements or enumeration of methodology would minimize the potential for regulatory arbitrage. Although there is a hearing process if a license is revoked or suspended, there is no other indication of an appeal or hearing process for other significant actions taken by the Department. We suggest that NYDFS include a broad and effective appeals process in order to ensure fairness and transparency throughout the licensing process.

Section 200.8(b) – Capital Requirements

This section provides NYDFS with nearly unfettered discretion as to capital requirements. Factors - but not methodologies, guidelines or ceilings - are provided. Moreover these factors are not applicable to many startups that maintain full reserves rather than leveraged assets. In the absence of defined guidelines, methodologies or other assurances as to adequate capital floors and ceilings, this discretion will impede regulatory clarity and certainty for market entrants and participants.



Section 200.8(a) – Bond

Again, like the capital requirements, the bond requirements are left to the discretion of NYDFS. We request that in the interests of transparency and regulatory clarity, the final regulations outline a reasonable floor or ceiling to provide entrepreneurs with clear guidelines and expectations that are risk-based.

Section 200.8(b) - Permissible Investments

This is another unusual provision under NY licensing laws. New York has long had requirements for “permissible investments,” which regulate how licensees must hold and invest funds/securities equal to the amount of customer funds being held (referred to as “outstanding payment instruments.”). It is reasonable to require restrictions on investments ensuring soundness of a firm and to prevent loss of consumer funds. But these proposed regulations purport to regulate how a licensed entity invests *its own* “retained earnings and profits.” While the restriction on investments may be good unsolicited business advice, it appears extraordinary to place legal restrictions on how these entities invest *their own* profits.

Once again, our members question why the Department has elected to impose more severe restrictions on digital assets businesses than on other licensed money transmitter businesses, particularly where small startups pose lower risk to consumers, and where technologies have enabled innovations such as multisignature wallets, proof of reserve audits, and continuous real-time accounting, do not expose customers, in many business models, to any risk of financial loss.

Section 200.9(b) – Custody and Protection of Customer Assets

Another departure from existing NY licensing laws is the requirement that, to the extent a licensee stores or holds digital assets on behalf of its customers, the licensee must hold what is effectively “permissible investment” in *the same type and amount of digital assets as that which is owed or obligated* to those customers. While this section has some basis due to the volatility of some digital currencies, this obligation should only apply to digital currency businesses that make storage or holding of digital assets a core service, as that is the only instance in which there is risk to customer funds. Some digital asset businesses offer exchanges that move various digital assets in and out quickly. It would be extremely difficult and in our view unnecessary to retain multiple reserves for each particular kind of digital asset that may be transmitted over the course of a day or week.



Section 200.10 – Material Changes To Business

This section requires permission – prior written approval - from NYDFS for “any plan or proposal to introduce or offer a new product, service, or activity, or to make a material change to an existing product, service, or activity, involving New York or New York residents.”

Not only does this provision have no time deadline for how quickly NYDFS must respond to requests for written approval, this imposes unacceptable restraints on how a licensed digital asset business must operate. This section also improperly allows NYDFS to pre-screen products for competitive purpose, and restrict competition by creating artificial barrier to bring products to market. Cases have demonstrated that larger, incumbent players typically have better access to regulators and faster approvals than smaller ones. A licensed digital assets business that has met the Department comprehensive financial, capital, and compliance requirements should not have all product innovations pre-approved as well. We suggest that at a minimum, this section be revised to require notification, not approval, of material changes within a reasonable amount of time.

Section 200.12 – Books and Records

This section sets forth requirements for books and records required to be maintained by the licensed digital asset business. Again, the list of requirements and the length of time such records should be maintained (ten years) seem to be quite burdensome and potentially unfeasible especially since there is no tier or other monetary value to trigger such record-keeping requirements. The collection of PII for both senders and recipients to a transaction is not feasible in decentralized open networks. We also note that the BSA requires retention of records for only five years. Further, the mass data collection without corresponding risk benefit is an impermissible invasion of financial privacy.

We urge NYDFS to take a deeper look at how the old “closed shop” model emerged in the era of closed “black boxes” of proprietary institutions, within the current context of new technologies that reduce or replace that model for better governance, AML and fraud prevention. With blockchain, there is a real-time, publicly available database that can be analyzed for suspicious activity; we no longer need to solely rely on private institutions to collect information, nor manually piece together that private collection, as we did in the 20th century.



By proposing massive expansion of data collection to market entrants and requiring PII to be held for ten years, NYDFS exacerbates the privacy problem without any corresponding benefit in trust, identity or risk reduction. We face inherent challenge in enabling counterparty trust on the Internet using current analog and documentary KYC methods. Credit cards, for example, were not originally intended for e-commerce but rather for point-of-sale purchases. Government issued photo IDs, in another example, were intended to verify identity using the photo on the card with the attributes of a physically present individual. Yet even today BSA/AML/KYC requirements are foundationally based on these pieces of “identity verification”. These pieces of personally identifiable data, along with the name, address or phone number associated with an account, are then passed along each the various nodes on the decentralized network of the Internet in order to secure a payment, with the very real possibility of comprised identity at each step along the way. As the recent massive data breaches at Target, Home Depot, Kmart and JP Morgan show, the continued practice in the e-commerce world of using of personal data collection to process payments, a practice that originated in a brick-and-mortar world, present serious dangers to privacy and control of our identities.¹⁷

However, the very family of encryption technologies that make Bitcoin possible also make it possible to protect privacy and provide more tailored and effective governance. The key takeaway for financial regulators grappling with the difficult challenge of swiftly reimagining and retooling old regulatory means to a decentralized world, is that identity technologies as well as computational resources have evolved to the point where it is now feasible to authenticate identities without revealing identities. Technologies can now enable computations to verify personal information without necessarily disclosing the person’s identity to third parties without probable cause.¹⁸ We urge NYDFS to carefully consider that adapting existing AML/KYC practices for decentralized technologies requires more than mere expansion of the existing model, but a re-tooling of how we ensure trust and privacy online.

Section 200.12 (c) – Abandoned Property

We were surprised to see reference to abandoned property laws in Section 200.12 (c):

¹⁷ Jake Swearingen, “Why the JP Morgan Data Breach Is Like No Other”, *The Atlantic*, October 3, 2014, available at <http://www.theatlantic.com/business/archive/2014/10/why-the-jp-morgan-data-breach-is-like-no-other/381098/> .

¹⁸ MIT/ID3 “21 Top Bitcoin and Digital Currency Companies Endorse New Digital Framework for Digital Identity, Trust and Open Data, (Press Release October 20, 2014), available at <http://www.marketwired.com/press-release/21-top-bitcoin-digital-currency-companies-endorse-new-digital-framework-digital-identity-1959159.htm>.



Records of non-completed, outstanding, or inactive Virtual Currency accounts or transactions shall be maintained for at least five years after the time when any such Virtual Currency has been deemed, under the Abandoned Property Law, to be abandoned property.

Whether and how digital assets will be treated under abandoned property laws is a topic that not been addressed by the New York legislature nor by the courts. To suggest that the status of digital assets has already been determined under NY Abandoned Property law appears to be premature.

Section 200.13 – Examinations

DATA notes that that the Superintendent also maintains wide discretion to examine a licensee. We believe that examination should have clear limitations, particularly as it relates to the limited-purpose examination of an out-of-state affiliate for the licensee’s financial condition, or safety and soundness practices.

Section 200.15(d)(1) - AML

A number of our members have observed that the Anti-Money Laundering provisions in this section far exceed what existing law requires by FinCEN.

For example, subsection (f) prohibits knowingly allowing a digital assets transfer or transmission if it will “obfuscate the identity of an individual customer or counterparty” effectively preventing the use of “tumblers” or ‘aggregators” – even for very small transactions. However, in some instances, the use of “tumblers” maybe beneficial, for example, to protect against identity theft, data security, cyber-predators, to voice dissent, or otherwise engage in constitutionally protected anonymous speech. DATA urges NYDFS to ensure that its regulations are consistent with constitutional protections. It is one thing to permit a narrow exception to financial privacy for public policy reasons, it is another to expand that exception into an unconstitutional prohibition on privacy. At a minimum, NYDFS should clarify that only unlawful obfuscation is prohibited, not legitimate methods for identity protection.

Other language (subsection d(1)) specifies that all parties in any digital currency transaction, no matter what the amount, must be identified by name and physical address. DATA notes would create the equivalent of a closed loop Bitcoin network in which transactions would only be allowed by wallet providers if the counterparty to any one user’s transaction was also a known person. This restriction would impede Bitcoin’s global interoperability, and fungibility of the currency would be threatened.



The NYSDFS must recognize that it is impossible and illegal to prevent individuals from using open-source software and decentralized networks like the Internet freely and privately. The prohibition against anonymous Bitcoin account-holders may severely damage Bitcoin’s usability for honest actors. NY consumers that naturally eschew the complete loss of privacy when transacting with “BitLicensed” entities would go to other, unlicensed entities, leaving these actors outside of the visibility of NYDFS and more vulnerable to consumer losses.

Another extremely burdensome obligation is the requirement to report *to the DFS* (not to FinCEN nor any other federal regulator), *within 24 hours* any transaction (whether or not it is “suspicious”) exceeding the equivalent value of \$10,000 in one day, by one Person. (200.15(d)(2). Again, this is an extraordinary requirement, and one that seems particularly unjustified where there is a public basis for every transaction recorded on the public ledger.

New York SAR filing requirement” in subsection (d)(3)(ii) imposes a SAR filing requirement on licensed digital assets businesses *even if the business has no similar obligation under federal law*.

We respectfully urge the Department to revise these regulations so that they do not create a separate, state-level financial crimes function that is appropriately FinCEN’s purview, and do not impose excessively more burdensome obligations than those under federal law.

Section 200.15 (g)(1) – Identification of accountholders

There is a need to clarify what constitutes “accountholder” in the digital currency world of multisignature wallets and private key custodianship. By imposing impossible reporting requirements on companies that cannot track identities of users outside of their platform, the only solution for these services may be to block the IP addresses of New York residents.

Section 200.18 – Advertising & Marketing

This section seeks to require all licenses to affix the following phrase on all marketing materials “Licensed to Engage in Virtual Currency Business by the New York State Department of Financial Services”. However, this proposed rules does not take into account 21st century marketing tools such as Twitter that are prevalent in this industry. In addition, clear, conspicuous, close-in-time notices may be more effective than a



blanket requirement intended for print advertising.

Section 200.19 – Consumer Protection

DATA believes in protecting and treating consumers fairly. We have a working group devoted to best practices in consumer protection and aim to publish our guidelines in the coming months, which we hope will serve as a model for the industry. The list of required disclosures under this section, however, appear excessive, and in particular, we believe that the requirement to provide, with each transactions, all terms and conditions associated with each transaction, to be burdensome and likely to confuse, rather than inform, the user.

Section 200.20 – Complaints

Similarly, we believe the requirement to provide to NYDFS within seven days any changes to complaint policy overbroad, burdensome, and exceeding obligations imposed by similar fiduciaries.

VI. Conclusion

Thank you for NYDFS’ initiative in engaging private and public stakeholders in this important dialogue around the risks, opportunities and governance of these emerging technologies, and providing us with this opportunity to provide our comments to the Proposed Rule. As you recently stated this summer regarding NY State’s agreement with Lyft, another disrupter of another centralized model, we, too are “firmly committed to the notion that regulators can work constructively with companies so that new ideas can come to the market - and that smart regulation should create an environment where innovators can compete.” We believe that NYDFS can strike the right policy balance. DATA stands ready to work with all stakeholders, and welcomes further discussion and engagement on these critical issues in the second round of comments.

Sincerely,

A handwritten signature in blue ink, appearing to read "Constance", is written over a light blue horizontal line.

Constance Choi

Founding Board Director & Secretariat, DATA