

Adam Ettinger  
Strategic Counsel Corp  
649 Mission St., 5th Floor  
San Francisco, CA 94105

Judith Rinearson  
Bryan Cave LLP  
1290 Avenue of the Americas  
New York, NY 10104

October 21, 2014

Mr. Dana Syracuse  
New York State Department of Financial Services  
One State Street  
New York, NY 10004-1511

Re: Comments on Proposed Rulemaking Regarding Regulation of the Conduct of Virtual Currency Businesses - DFS-29-14-00015-P (“**Proposed Regulations**”)

Dear Mr. Syracuse:

Thank you for the opportunity to provide our comments in response to the Department’s proposed BitLicense reflected in the Proposed Regulations. We are attorneys<sup>1</sup> who work extensively in the areas of cryptocurrencies such as Bitcoin, digital currencies, prepaid cards and other banking and payment systems. We are submitting this comment letter jointly, not on behalf of any particular client, but to further the benefits that cryptocurrency<sup>2</sup> products and their developers represent for our future, and to help ensure the growth and stability of such products through reasoned, balanced, and thoughtful regulation.

As an initial comment, we commend the Department for its efforts, and we understand the difficulty that the Department faces when trying to draft regulations for cryptocurrency platforms. This

---

<sup>1</sup> Judith Rinearson is a Partner at the New York City offices of Bryan Cave LLP. An authority in the area of prepaid and emerging payments, Ms. Rinearson has practiced law in the emerging payment area for more than 20 years. In addition, Ms. Rinearson testified before the Department on January 28, 2014. See <http://www.bryancave.com/judithrinearson/>

Adam T. Ettinger practices at the law firm Strategic Counsel Corp. as its managing partner. Mr. Ettinger counsels technology companies in formation, financing, technology development, privacy, intellectual property transactions, and commercial contracts. In the last few years, his practice has focused on new ventures in the cryptocurrency ecosystem, including Bitcoin security developers, mining equipment manufacturers, exchanges, payment service companies, and investors. Mr. Ettinger has also had the privilege of representing leaders in semiconductors, networking technology, social gaming, internet advertising, and mobile apps, including AMD, Apple, DeviceScape, Intel, Lucrative Gaming (fgl), Magma Design, Network Solutions Inc. (NSI), Orchestra (acquired by CA), S3 (acquired by HTC), Self Aware Games (acquired by Big Fish), Social Concepts, and Undertone Networks.

<sup>2</sup> While we see the benefits of virtual currencies generally, we believe that Bitcoin and other similar cryptocurrencies appear to offer the greatest promise. They are distinguished by the following factors: cryptographic authentication, cryptographic verification of transactions by a network of volunteered computers, and a decentralized and publicly accessible ledger such as Bitcoin’s blockchain. Because they have no centralized control over the operation of the enabling protocols, they are less susceptible to centralized attacks or to the technical incompetence of a single, central developer of the protocol, and therefore arguably less needy of regulatory oversight.

is particularly true for platforms that require no intermediaries between counterparties, and allow transactions directly between individuals who are able to trust the transaction even if they share no personal information when consummating the transaction.

The Department has received many responses that focus on the difficulty, costs and uncertainty that the respondents believe they will struggle with should the Proposed Regulations be adopted as drafted. We wish instead to focus on the deleterious impact we would expect the Proposed Regulations to have on New York residents, businesses, and community of technology start-ups and their investors. We have come to the conclusion that adopting the Proposed Regulations as currently drafted would undermine its objectives: to protect consumers, enhance security and prevent money laundering. We come to these conclusions based on our experience with financial regulations, our understanding of the technologies, our experience observing how the venture finance community and their portfolio companies have navigated earlier regulatory efforts, and our conversations with investors and companies in the cryptocurrency ecosystem. We hope that our comments will assist the Department in revising and finalizing regulations that will allow the safe and secure growth of the cryptocurrency ecosystem.

We suggest below several revisions and recommend different approaches, mindful that the Department has already received many thoughtful and well-articulated responses to the Proposed Regulations.

## **I. Unintended Consequences of the Proposed Regulations**

Recognizing that the intentions of the BitLicense is to benefit consumers, the financial system, the cryptocurrency ecosystem, and the State of New York, we first note three major concerns arising out of the Proposed Regulations.

### **A. Increased Vulnerability to Cybercrime.**

The Proposed Regulations would require each licensee to acquire, retain and share with the Department more highly-confidential, non-public, personal information than any other similar federal or state regulations have required of financial services or technology companies previously. Requiring this collection and retention of so much sensitive personal information will make BitLicense applicants and licensees, many of which will be newly formed, technology start-up companies, the targets of global cybercrime. No doubt licensees will strive to adopt the highest levels of cyber security. However, such efforts did not avail many other large, established and highly respected entities, such as JPMorgan Chase, which was recently the victim of a cyber-security breach that reportedly compromised the accounts of 76 million households and seven million small businesses.<sup>3</sup> The news is regularly filled with the names of other corporations whose cybersecurity was breached despite extensive, expensive and exhaustive security programs: Home depot, Target, Ebay, Adobe, and others.

The types and range of data that the Proposed Regulations require to be collected is also concerning given recent developments in mobile payment systems and hacking. Section 200.4 of the Proposed Regulations would require each applicant to collect a set of completed fingerprints and photographs from *each* employee, Principal Officer, Principal Stockholder, and Principal Beneficiary (as

---

<sup>3</sup> [JPMorgan Chase Hacking Affects 76 Million Households New York Times, October 2, 2014.](#)

each is defined in Section 200.4).<sup>4</sup> Although there is precedent for requiring fingerprints from money transmitter licensees, the risks of doing so has greatly increased this week. Yesterday, Apple launched Apple Pay, a mobile payment service that lets iPhone owners pay for goods and services and authorize credit card payments using their fingerprints and Apple's Touch ID.<sup>5</sup> Other mobile device manufacturers will no doubt follow Apple's lead and offer competing fingerprint authentication. Banking and payment apps utilizing fingerprint authentication will no doubt proliferate in the coming months and years. Touch ID was hacked when first launched and reportedly remains vulnerable if the criminal can obtain copies of fingerprints.<sup>6</sup>

BitLicense licensees may strive to the highest security standards despite being new ventures, but the difficulties are enormous. We believe that the future of financial regulations should focus on ways to *reduce* the collection of personal information in order to *increase* consumer protection. Bitcoin and similar distributed ledger protocols have engineered just that. The Proposed Regulations would negate this protection, and every cybercriminal would know that the best treasure-troves of personal information are held by licensees of the New York BitLicense, including biometric information that the cyber-criminal would find it hard to get elsewhere.

Not only do many states restrict the amount of data being collected from consumers, the European Union Data Privacy Directive<sup>7</sup> and related laws and regulations also impose significant requirements on companies in the EU before they may share the types of information required under Section 200.4, including explicit affirmative consent of the individual affected. Most companies seeking a BitLicense will do so only after initial formation, hiring developers and executives, and closing initial capital investments. If any of the investor or employees do not give their affirmative consent to such broad disclosures of personal information (together with the signatures and fingerprints required) and live in the EU or similar jurisdictions with privacy protections, then the company may have no choice but forego the BitLicense and New York.

## B. Certain Data Collection Requirements are Impractical or Impossible

Even if there were no cyber crime threats hanging as a Sword of Damocles above the heads of the cryptocurrency industry, the simple act of collecting and storing the data required under the Proposed Regulations is extraordinary and daunting. Section 200.12(a)(1) of the Proposed Regulations would

---

<sup>4</sup> Further, Section 200.4 would require each applicant to collect for each director Principal Officer, Principal Stockholder, and Principal Beneficiary: the individual's name, address, information and documentation regarding their personal history, experience, and qualifications; a background report prepared by an independent investigatory agency; a form of authority signed by such individual (i.e. with the person's signature); a current financial statement for the applicant and each Principal Officer, Principal Stockholder, and Principal Beneficiary of the applicant; and disclosure of banking relationships.

<sup>5</sup> <http://www.apple.com/apple-pay/?cid=wwa-us-kwg-features-com>.

<sup>6</sup> Days after Apple introduced fingerprint locks on its phones, a group showed how they could be hacked. See, <http://www.infoworld.com/article/2612237/apple-phone/video--iphone-5-s-fingerprint-scanner-hacked-already.html>. Shortly after the iPhone 6 was introduced, this was repeated. (See, <https://blog.lookout.com/blog/2014/09/23/iphone-6-touchid-hack/>). The researcher considers it difficult to lift a fingerprint off of a shiny surface, and therefore unlikely that common criminals will take the effort to do so to hack the TouchID authentication. However, one must consider that it would not be that difficult to print an accurate fingerprint using pilfered fingerprint records. 3D printers have printed human tissue for years, and such 3D printers are now considered mainstream and "off the shelf". More sophisticated 3D printers are becoming able to printing entire organs. See, <http://www.theguardian.com/science/2014/jul/04/3d-printed-organs-step-closer>, and [https://www.ted.com/talks/anthony\\_atala\\_printing\\_a\\_human\\_kidney](https://www.ted.com/talks/anthony_atala_printing_a_human_kidney).

<sup>7</sup> Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

require licensees to collect and maintain for ten (10) years books and records that include, “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[.]” Other respondents have commented on the difficulty and practical impossibility of this requirement. The Bitcoin protocol and other virtual currency protocols simply do not have the ability to store and transmit such information any more than the protocol used by VISA can include a 3D life-like avatar of each credit card holder. In effect, the Proposed Regulations would require cryptocurrency companies to do what is not feasible, and abstain from offering customers the privacy they increasingly wish was available to shield them from the identify theft and personal information data breaches.<sup>8</sup>

### C. A Long-Term Negative Impact on the New York State Crypto Currency Industry

We are also very concerned about the unintended impact that we believe the Proposed Regulations will have on the nascent New York cryptocurrency industry. The difficulty, risks, costs and uncertainty of compliance are already leading some cryptocurrency companies to look elsewhere for a U.S. base.

For example, venture capitalists have invested over \$250,000,000 in cryptocurrency companies in 2014. We find it telling that none of the significant investments made after publication of the Proposed Regulations were in New York. Bitcoin Opportunity Corp. is the most prominent a New York venture fund focused on the cryptocurrency ecosystem. It invested in one New York company the day before the Proposed Regulations were published. Since then it has made nine investments. Not one was in a company based in New York.<sup>9</sup> Sadly, we understand that soon after the publication of the Proposed Regulations, investors and entrepreneurs nation-wide read the published assessments of the Proposed Regulations and began to explore how to make geo-fencing New York a priority.

New York financiers are not the only ones that may find themselves with fewer local opportunities. While the Proposed Regulations seek the laudable goals of consumer protection and preventing money laundering, the proposed regulatory burdens will severely diminish the number of companies that could otherwise serve New York’s unbanked and underbanked populations.<sup>10</sup>

If the Department wanted a panoply of solutions for the unbanked and underbanked, the cryptocurrency ecosystem appears made-to-order and its community strongly espouses these objectives. Unlike traditional banks and other financial service companies, Bitcoin and other cryptocurrencies were designed to incorporate and extend the most recent innovations in peer-to-peer networking and mobile communications. Bitcoin start-ups are staffed by the best and the brightest talent in mobile technology and marketing, trained at making products simpler and more usable. Fortunately, the underbanked are *more likely* to have a smart phone than households that are fully banked.<sup>11</sup>

---

<sup>8</sup> Although reported breaches at large companies such as Target and Home Depot make the news, many do not. See, e.g., [http://www.idtheftcenter.org/images/breach/IIRC\\_Breach\\_Report\\_2014.pdf](http://www.idtheftcenter.org/images/breach/IIRC_Breach_Report_2014.pdf).

<sup>9</sup> Source: CB Insights.

<sup>10</sup> On a national average, over one quarter of all households are unbanked or underbanked according to the 2011 FDIC National Survey of Unbanked and Underbanked Households. According to Prof. Lisa J. Servon, in 2013, the South Bronx had only one bank per 20,000 residents, whereas in Manhattan, one bank served every 3,000 residents.

<sup>11</sup> 2013 FDIC National Survey of Unbanked and Underbanked Households.

The cryptocurrency community suffered deep disappointment after the Proposed Regulation were published because they believed that their companies and their investors who wanted to serve the unbanked and underbanked, would not be able to absorb the regulatory cost, risk, effort and uncertainty.

Unintentionally, the Proposed Regulations may have also added fuel to efforts to create alternatives to Bitcoin designed to allow users greater anonymity,<sup>12</sup> and allow bad actors to evade regulation and prevent regulators and the public from benefitting from the transparency encoded into Bitcoin's blockchain. It is this transparency (whereby anyone anywhere in the world, at any time and without any cost, can see all transactions) that provides the very protections our financial system needs.

## **II. Suggested Changes to the Proposed Regulations**

In addition to our three over-arching concerns, we have several specific suggestions for changes to the Proposed Regulations.

### **A. Make Appropriate Use of Existing State Money Transmitter Licensing Laws**

New York has a robust, well defined, set of money transmitter licensing laws that have withstood the test of time.<sup>13</sup> Except for a few areas that can be addressed through customized amendments, we see no reason why cryptocurrencies cannot be quite effectively and efficiently regulated through existing money transmitter laws.

- The services provided by cryptocurrencies are correlate closely to those provided by traditional money transmission products: person-to-person remittances, international remittances, online payments and payments at the point of sale, secure payment instruments, etc.);
- The risks posed by cryptocurrencies are also quite similar to those posed by traditional money transmission products: money laundering, loss due to mishandling or mismanagement, and use for financial crimes such as fraud;
- The infrastructure for licensing and enforcement of money transmitter laws are already in place; and
- Since cryptocurrencies often compete with traditional licensed money transmission products, using the same regulatory framework for both would ensure a level playing field for all.

One of the many advantages to this approach is that attorneys can give their technology clients and prospective investors a better idea of what is required to obtain a license, in cost, timing and effort. If the Proposed Regulations is adopted, establishing a wholly new licensing regime, attorneys will have no case precedents or enforcement history with which they can give their clients a well-based estimate of the costs, timing and effort required to obtain a license or comply with the regulations. The only thing that

---

<sup>12</sup> For example, Darkcoin, Dark Wallet and Zerocoin.

<sup>13</sup> Transmitters of Money (N.Y. Banking Code, Article 13-B, § 640 et seq.)

the venture capital community detests more than regulations are regulations that are uncertain, greatly affect budget, product development, and customer acquisition.

We agree with other commenters that adding *certain* virtual currency businesses to the list of licensed money transmitters under existing law makes good sense and believe this can be done easily, with minor changes to bonding or permissible investment requirements specific to cryptocurrencies.

If the Department wishes to continue to have a separate BitLicense licensing scheme for cryptocurrency companies, then the regulations should take great care not introduce greater regulatory burdens than those applied to licensed money transmitters in New York.

**B. Reduce the Collection of Personal and Biometric Information; Maintaining a Level Playing Field**

New York's money transmitter licensing requirements do not impose fingerprinting on every employee. Nor do they require organizational charts with "lines of authority" and "allocation of duties". These are just two examples of some of the overly onerous application requirements made applicable solely to cryptocurrency businesses. We urge reconsideration and a more even-handed approach to cryptocurrency businesses so that your applicants have less risk of security breaches, and more ordinary regulatory burden in this regard.

**C. Define "Virtual Currency Business Activity" Narrowly to Reflect Only What is Needed to Ensure Protection of Public Safety in New York**

The Proposed Regulations define "Virtual Currency" with unnecessary breadth.<sup>14</sup> Other respondents to the Proposed Regulations have addressed aspects of this issue. However, we wish to note in particular the definition in subsection (2) which states: "securing, storing, holding, or maintaining custody or control of Virtual Currency on behalf of others." We understand why "control" is a factor, but it begs the question, what is "control" when it comes to cryptocurrencies? At least with respect to Bitcoin and similar cryptocurrencies, we suggest that "control" should be defined to mean that the person or business can transfer the cryptocurrency from a wallet address that is not theirs to another wallet address on behalf of the owner of the cryptocurrency without any cryptographic authentication provided directly by the owner of the cryptocurrency. This would give an exception to Bitcoin security providers that, through hosted or API services, wish to provide multi-signature authentication to consumers and businesses. If the security provider wants to make a New York resident's cryptocurrency holdings more secure, and cannot maliciously or accidentally transfer the holdings, then such security providers should not be disincentivized by the licensing requirements from bringing security solutions to New York residents.

---

<sup>14</sup> "Virtual Currency Business Activity means the conduct of any one of the following types of activities involving New York or a New York Resident:

- (1) receiving Virtual Currency for transmission or transmitting the same;
- (2) securing, storing, holding, or maintaining custody or control of Virtual Currency on behalf of others;
- (3) buying and selling Virtual Currency as a customer business;
- (4) performing retail conversion services, including the conversion or exchange of Fiat Currency or other value into Virtual Currency, the conversion or exchange of Virtual Currency into Fiat Currency or other value, or the conversion or exchange of one form of Virtual Currency into another form of Virtual Currency; or
- (5) controlling, administering, or issuing a Virtual Currency."

For the same reasons, the word “securing” should be deleted from the definition in subsection (2). If a company can secure cryptocurrency holdings without the technological ability to abscond with them, then it does little good to impose upon them the choice between withholding security from New Yorkers and the burden of becoming licensees. We discuss security technology further in Section II(F) below.

The words “storing, holding, or maintaining custody” in subsection (2) should be also stricken because they apply antiquated notions of control on cryptocurrencies that lead to unintended applications of the definition. A person can print out his or her private key and place it in a deposit box or leased storage unit along with other personal papers and old furniture. Does this make either the bank or the storage company one that engages in a “Virtual Currency Business Activity”? We would hope not. Similarly, a number of cloud-based services allow electronic document storage in the “cloud” with or without encrypted access. If the user stores his or her private keys there, it would seem that the definition would require the cloud storage company to know what documents are kept on its servers and to get a BitLicense.

However, if a company stores, holds or maintains custody of private keys of a cryptocurrency wallet on behalf of a customer, and its business and can *control* the cryptocurrency (i.e. can transfer it without the customer’s separate cryptographic signature) then that company already falls in the definition of conducting Virtual Currency Business Activity. The words “storing, holding, or maintaining custody” are unnecessary. Moreover, the word “custody” only adds confusion. What does it mean to have custody over a Bitcoin wallet that it cannot control? Indeed, can it truly have custody over a Bitcoin wallet that the customer still controls? The nature of cryptocurrencies doesn’t lend itself to the language of bailment.

#### D. Clarify the Exemption for Merchant Payment Processors

Section 200.3(c)(2) should provide an exemption for merchant payment processors as they pose little risk to consumer protection or of money laundering. To process cryptocurrency payments made by consumers for goods or services, payment processors often need to convert the cryptocurrency into fiat currency that is then paid to the merchant in settlement. However, such is not an exchange business that might then give the fiat currency to a money launderer. Further, merchants are in a good position to choose a professional, stable and reliable payment processor from the myriad of alternatives. Another approach would be to exclude payment processors unless they process purchases for amounts greater than \$10,000 (or some other threshold) from customers in New York, especially if they are not registered with FinCEN.

Other respondents have sufficiently addressed issues in the other subsections of this definition, and so we find no need to do so here.

#### E. Restrictions on Licensee Investments and Business Changes Are Unworkable.

Currently licensed money transmitters are not required to invest their own profits in a narrow range of investments, nor are they required to obtain approval before launching any new product or service. Were they required to do so, New York would see an exodus of money transmitters from New York. We believe that investors will not invest in a technology start-up in New York or allow their portfolio companies to do business in New York if the investors think that any product launch, product update, service modification or business “pivot” must be approved or pre-approved by the Department.

We cannot say for certain, because no regulations have sought these requirements from technology ventures in the past. The definition of “material change” is hardly comforting because it is hardly limiting. Instead, it manages to be both extensive and ambiguous. Moreover, swift product and business changes are often needed to *fix* a product or service and make it *safer* for customers. Prior approval by the Department would require a licensee to keep the faulty product in place and/or continue to provide faulty services until the Department could review and approve the proposed changes.

#### F. Security Providers as Consumer Protection

The Department no doubt desires the best security companies to protect the financial accounts and transactions of companies and individuals in New York. Unfortunately, the Proposed Regulations could have the opposite effect. Section 200.2(n) broadly defines the activities that will subject a company to the BitLicense regulations and oversight by the Department, and includes any company that *secures virtual currency* on behalf of others.<sup>15</sup> Several companies have already made using Bitcoin much safer for consumers, for example, by providing authentication services (such as two-factor authentication), or enhanced wallet security (such as a multi-signature wallets). We are concerned that Section 200.2(n) would force companies that develop hosted security technologies in order to protect virtual currency consumers to choose between: (a) sharing that technology with New York residents and undergoing the difficulty, cost, and uncertainty of applying for a BitLicense, and (b) avoiding New York and its residents.

Ironically, these are the companies that have improved consumer protection. Only one year ago, the greatest fear voiced by consumers and the press was that if a person lost his or her private key, or if a hacker stole it, the Bitcoin would be lost forever. BitGo launched multi-signature wallets after extensive development to eliminate these problems.<sup>16</sup> Other companies have followed. No BitGo wallet has yet to be hacked. As another example, Authy and other companies offer two-factor authentication to secure Bitcoin wallets held by customers of Coinbase, BitGo and others. Even if a hacker steals a user’s private key or password, two-factor authentication prevents the hacker from gaining access to the account unless the hacker also steals the user’s phone or can commandeer the user’s phone account. More companies have been financed, and will develop products and services that secure and protect a consumer’s holdings. Requiring them to become regulated entities with intensive compliance requirements will limit the services being offered to New York companies and consumers.

We understand from Mr. Lawskey’s discussion at Cardozo Law School last week that the Department still sees an important distinction between offering security software (i.e. a file someone can download) and a company making such software available on a hosted basis. However, it is the distinction of *control* that we find important, as discussed in Section II(C) above. Otherwise, New York residents and businesses will need to try to find downloadable software analogs of multi-signature wallets and other security software that will be more difficult for ordinary people to find, download, install, configure and use properly compared to hosted versions.

#### G. Cyber Security

---

<sup>15</sup> “*Virtual Currency Business Activity* means the conduct of any one of the following types of activities involving New York or a New York Resident [ . . . ] securing, storing, holding, or maintaining custody or control of Virtual Currency on behalf of others[.]”

<sup>16</sup> BitGo, Inc. is a client of Strategic Counsel Corp.



The requirements of section 200.16 are not unreasonable -- but to ensure a level playing field, these should apply to all money transmission businesses. Doing so would also increase the number of consultants and vendors with common expertise that can help implement and maintain cyber security programs. Doing so would also ensure that guidance from the Department and enforcement actions would reach a larger, common audience. Recent events illustrate that no business is immune from cybercrime. We understand from Mr. Lawsky's comments at Cardozo Law School that the Department is contemplating extending such obligations to other entities holding sensitive consumer data.

#### H. Start-Up Safe Harbor/Phased-In Approach

Cryptocurrencies open doors to a multitudes of new and emerging businesses and payment products. As others have suggested, we believe a tiered approach that allows smaller, start-up companies to launch their businesses without having to fulfill complete licensing obligations should be an option, provided that the start-up companies limit their business to low risk products. Again, we acknowledge that Mr. Lawsky noted in his Cardozo Law School presentation the difficulties in carving out a safe harbor for start-ups but that nevertheless he indicated that the Department would take steps to address that issue. We applaud that effort.

#### I. Leave Anti-Money Laundering ("AML") Regulation to FinCEN and The Federal Regulators

FinCEN, the federal agency tasked with the job of preventing financial crimes such as money laundering and terrorist financing, has issued guidance<sup>17</sup> on how cryptocurrencies are to be regulated under the Bank Secrecy Act. These are matters of national security and this the core of FinCEN's mission. While it makes complete sense to require all licensed cryptocurrency businesses to have an effective AML compliance program that complies with applicable federal AML laws and regulations (just as licensed money transmitters are so required), in our view it is unnecessary, inappropriate and not really fair to add an additional layer of state AML laws that do not apply outside New York and do not apply to traditional money transmission products. We suggest that the separate section on AML compliance be deleted and that existing federal law apply instead.

### III. Concluding Comments

In addition to re-considering the Proposed Regulations for the BitLicense, the Department may wish to consider amending other regulations to foster innovations in cryptocurrency services rather than restrict the cryptocurrency ecosystem from growing and thriving. As the Department knows well, money transmitters have difficulties obtaining ordinary bank accounts. A company involved in Bitcoin finds it nearly impossible. Perhaps it would help cryptocurrency companies with New York offices to obtain bank accounts if regulations were amended to exempt banks under New York State laws from any direct or derivative liability for the actions of a BitLicensee (or its customers) merely because the bank furnished the bank account. Such exemption from liability could be conditioned upon the bank conducting adequate due diligence of the licensee's onboarding procedures for its customers. In other words, to attract the most promising cryptocurrency companies to New York and investment in those

---

<sup>17</sup> See FIN-2013-G001, "Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies" (March 18, 2013).

companies, perhaps there is more that the Department or other departments can do to ease the current difficulty these companies have.

Many compare the advent of cryptocurrencies equal only to that of the invention and commercialization of the internet itself. The comparison is helpful. Although email was misused by con artists and other criminal elements, yet, with the advantage of hindsight, we can see that the benefits provided far outweighed the threats and damages done by bad actors. Miracles, like a college student vetting auto mechanics on Yelp, or a grandmother being able to videoconference with her granddaughter for free each Sunday morning, only occur because state and federal agencies were wise enough to minimize regulations, or proactively create safe-harbors where new ventures could germinate, grow and thrive.

The very best and the brightest technologists, entrepreneurs, and investors have congregated around Bitcoin and blockchain technologies because they see the opportunity to create a new batch of miracles. As we write this, they sit in boardrooms and coffee shops strategizing where and how to focus their efforts. At the top of their list of concerns: the regulatory environment that the New York Department of Financial Services has in its hands. Allow it to thrive in New York, and the cryptocurrency ecosystem will build solutions to the concerns voiced now by the Department, just as eBay built solutions to fraud between purchasers, and BitGo built a solution to private key loss and theft. Let the ecosystem thrive, and it will create solutions that regulations and enforcement efforts cannot achieve.

To conclude, we believe the regulatory efforts represented by the Proposed Regulations can be the key to Bitcoin and other cryptocurrencies' successful and beneficial growth and development. But they can also lock out new ventures if the regulations are not approached with a very light hand and a balanced and reasoned focus. We hope our comments are helpful and would be happy to spend further time or answer your questions as needed.

Sincerely,



Judith Rinearson



Adam T. Ettinger