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

Peter Van Valkenburgh, Harley Geiger, and Berin Szoka

New York Department of Financial Services
Submitted October 21, 2014

On July 17, the New York Department of Financial Services (the Department) released a proposed regulatory framework for Virtual Currency businesses, called "BitLicense." Superintendent Benjamin M. Lawsky and the Department deserve congratulations for their foresight and willingness to engage this complex issue. New York has maintained a preeminent position in global financial markets for centuries. Given that history, we urge the Department to tread carefully in regulating Virtual Currency, because the policies New York establishes will have a broad impact. Unfortunately, as written, the BitLicense would severely harm user privacy and create major obstacles to innovation. Virtual Currency technology has the potential to unleash a new class of innovative products and services, and it would be profoundly unfortunate if Virtual Currency innovators, investors, and users were inhibited by onerous and harmful regulations issued by the Department.

Coin Center, The Center for Democracy and Technology, and TechFreedom, jointly submit these comments to the Department's rulemaking with the aim of protecting user privacy, business certainty, and innovation. Coin Center is a new non-profit research and advocacy center focused on the public policy issues facing digital currency technologies. The Center for Democracy and Technology (CDT) is a non-profit public interest organization focused on privacy and other civil liberties issues affecting the Internet, other communications networks, and associated technologies. CDT represents the public's interest in an open Internet and promotes the constitutional and democratic values of free expression, privacy, and individual liberty. TechFreedom is a non-profit, non-partisan technology think tank. Focusing on issues of Internet freedom and technological progress, TechFreedom works to protect innovation and discovery from powers that fear change. TechFreedom believes technology is the great driver of social progress and human well-being — and aims to keep it that way.

INTRODUCTION

Several excellent comments have been filed in this proceeding, many of which focus on how the proposed BitLicense can be adjusted in order to preserve freedom to innovate in the Virtual Currency space.[1] Seeking not to repeat these arguments, Coin Center, the Center for Democracy & Technology (CDT), and TechFreedom wish to focus this comment largely on the important issue of financial privacy as it relates to

[1] *See e.g.*, Jerry Brito and Eli Dourado, *Comments to the New York Department of Financial Services on the Proposed Virtual Currency Regulatory Framework* (Mercatus, Aug. 2014) *available at* http://mercatus.org/publication/comments-new-york-department-financial-services-proposed-virtual-currency-regulatory.

digital currencies, and on certain modifications to the BitLicense proposal that would enhance the security and privacy of Virtual Currency users.

The proposed BitLicense already includes several provisions that will enhance privacy and security services provided by Virtual Currency firms. Specifically, we recognize the value of sections 200.16 and 200.7(c) in requiring licensees to establish cyber security and privacy programs.

As presently drafted, however, the benefits of these regulatory requirements are largely offset by other provisions in the Department's proposed BitLicense. These provisions would be detrimental to the privacy of Virtual Currency users, create new liabilities and security risks for Virtual Currency companies and their affiliates, and would chill security-enhancing innovations. We urge the Department to reconsider these provisions to ensure its regulations benefit the users, providers, and thought-leaders of future financial technologies.

To that end, we have six primary recommendations, summarized here and explained in depth below:

1. **Do not require a record of the identity and address of every party to each transaction.** The requirements of § 200.15(d)(1) would compel a broad range of services to record, among other information, the identity and physical address of every party to a Virtual Currency transaction. Such a recordkeeping requirement goes well beyond the existing requirements for traditional money transmitters,[2] placing onerous technical and administrative burdens on Virtual Currency innovators while also creating undue privacy and cybersecurity risks. For most transactions, the BitLicense should not require service providers to record or share the identity of those parties that are not their own customers.[3]

2. **Exclude individual uses from "Virtual Currency Business Activity."** The proposed definition in § 200.2(n)(1) is overbroad and encompasses purely individual, personal uses of Virtual Currency. Mandating recordkeeping and reporting from individual users directly curtails their financial privacy, may deter individual use of Virtual Currency, and may also violate the individual user's constitutional rights—with dubious corresponding benefit. This definition should be narrowed to focus on services with full custodial control of Virtual Currency, excluding most uses in which the individual owner is in control of the Virtual Currency.[4]

3. **Exclude ancillary services from "Virtual Currency Business Activity."** The proposed definition in § 200.2(n)(1)-(2) would encompass ancillary services with no control of the Virtual Currency. As a result, the extensive recordkeeping requirements elsewhere in the BitLicense apply to an unnecessarily large number of diverse businesses and users. The definition should exclude ancillary services that merely "secure" or "transfer" Virtual Currency, but which do not have custody of the currency, such as cybersecurity services and electronic networks. The definition should also more clearly exclude online gaming currency from the recordkeeping requirements.[5]

4. **Exclude decentralized currency issuers from "Virtual Currency Business Activity."** The proposed definition at § 200.2(n)(5) would potentially encompass the "miners" and open-source

[2] *See* 31 C.F.R. §§1022.400 and 1010.312.
[3] *See infra* pp. 7-9.
[4] *See infra* pp. 9-12.
[5] *See infra* pp. 12-13.

software developers unique to *decentralized* virtual currencies. The proposed BitLicense would impose intrusive recordkeeping requirements on these entities even though decentralized currencies are transparent by design and have no central administrative authority with control over how the currency is used.[6]

5. **Permit most users of Virtual Currency to obfuscate their identities.** Section 200.15(f) forbids businesses holding a BitLicense from permitting the transfer of Virtual Currency if the transfer would obfuscate an individual user's identity. This implies that Licensees must monitor their service to prevent such obfuscation, and at times forbid customers from using their own Virtual Currency. The default state of many digital currencies includes fully transparent, public transaction records, called block chain ledgers. 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.[7]

6. **Bring Suspicious Activity Reporting on par with current federal law**. At § 200.15(d)(3)(ii), Suspicious Activity Reports should not be required of Virtual Currency businesses when the activity does not rise to the requisite level for scrutiny under federal law. Suspicious Activity Reporting requirements should be no more stringent for Virtual Currency transactions than for transactions involving other types of currencies. [8]

In order to emphasize the need for these adjustments, this comment describes the privacy strengths and weaknesses of Virtual Currencies, as well as changes to the BitLicense proposal that would preserve these strengths and encourage innovations to remedy the weaknesses.

I. VIRTUAL CURRENCY FOSTERS FINANCIAL PRIVACY

The privacy-enhancing features of digital currencies can benefit consumers and businesses in several ways. Importantly, features of Virtual Currencies have the potential to mitigate the risks associated with poor financial privacy and security, including, (1) direct costs from identity theft and fraud; (2) chilling costs from activities forgone because of fears of public discovery; and (3) compliance costs incurred by merchants or intermediaries. The Department should modify its proposed BitLicense to avoid outlawing or seriously weakening these features to the detriment of consumer safety and crime-prevention.

A. Mitigating Direct Costs

The Bureau of Justice Statistics estimates that identity theft cost Americans over $24.7 billion in 2012.[9] That's $10 billion more in losses than all other property crimes combined.[10] Eighty five percent of thefts involved the unauthorized use of existing financial accounts — a direct consequence of poor financial security.[11] That year alone, 7.7 million people experienced the fraudulent use of a credit card and 7.5 million

[6] *See infra* pp. 13-15.
[7] *See infra* pp. 15-16.
[8] *See infra* p.16.
[9] *See* Bureau of Justice Statistics, *Data Collection: National Crime Victimization Survey (NCVS)* (2012) *available at* http://www.bjs.gov/index.cfm?ty=dcdetail&iid=245.
[10] *Id.*
[11] *Id.*

more experienced the fraudulent use of a debit card.[12] Some 34.2 million individuals, over 14% of the adult U.S. population, reported having suffered one or more incidents of identity theft in the past.[13]

Recent data breaches at major retailers[14] and financial institutions[15] showcase risks inherent in the retention of consumer financial data by intermediaries. In the case of the Target breach, hackers targeted a vulnerable server accessible to a heating and cooling company that Target used as a vendor.[16] By granting some network access to this vendor, Target unknowingly and unintentionally exposed the payment network to which its customers belonged.[17] With enough new and variable links in a chain, one is likely to be weak enough to unravel the whole.

Virtual Currencies can mitigate these risks by substantially reducing the number of parties that the consumer must trust with her personal data, as compared with credit card transactions. There is no card issuer because digital currencies (or, more accurately, the cryptographic key indicating ownership of Virtual Currency) can be held personally with one's phone, computer, or even a secret scrap of paper.[18] There are companies that make it easier for merchants to receive Virtual Currency,[19] though these intermediaries (unlike merchant acquirers for credit cards) do not need to take or retain any customer data that could be used by hackers or intrusive marketers.[20] Finally, merchants themselves need never take personal data in order to accept a Virtual Currency payment, much as brick and mortar merchants that accept cash need not keep a record of customer names, addresses, or financial account numbers.[21] With fewer vulnerable links in a payment chain, the risk of breach can be reduced and the direct costs of identity theft can be limited.

Virtual currencies do pose some consumer risks of their own.[22] The user's personal devices and online accounts can be compromised, and stored Virtual Currency can be stolen.[23] These possibilities create new dangers not typically present in previous payment systems. A credit card company would potentially refund amounts lost by the fraudulent charges of a hacker, but cryptocurrency is like cash in this regard: it will not be easily returned once stolen from a wallet.[24] Users should be made aware of this risk, and companies should enact safeguards to protect against theft of the currency.[25]

---

[12] *Id.*
[13] *Id.*
[14] *See* Robin Sidel, "Home Depot's 56 Million Card Breach Bigger than Target's," *Wall Street Journal* (Sep. 2014) http://online.wsj.com/articles/home-depot-breach-bigger-than-targets-1411073571.
[15] *See* Elizabeth Weise, "Citi, E*Trade attacked by JPMorgan hackers, reports say," *USA Today* (Oct. 2014) http://www.usatoday.com/story/tech/2014/10/08/citigroup-etrade-jpmorgan-hackers/16923659/.
[16] *See* Brian Krebs, "Target Hackers Broke in Via HVAC Company," *KrebsonSecurity* (Feb. 2015) http://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/.
[17] *Id.*
[18] *See* Blockchain.info, "Practical Paper Wallets," https://blockchain.info/wallet/paper-tutorial (last accessed Oct. 15, 2014).
[19] *See e.g.*, Bitpay, "Features," https://bitpay.com/features (last accessed Oct. 15, 2014).
[20] Richard Gendal Brown, "Lessons from Bitcoin: Push Versus Pull" *Thoughts on the future of finance* (Oct. 2013) http://gendal.wordpress.com/2013/10/21/lessons-from-bitcoin-push-versus-pull/.
[21] *Id.*
[22] *Id.*
[23] It's important to note that this is not a new vulnerability; online and mobile banking apps made end-user devices attractive targets for hackers long ago.
[24] *See* Gendal, *supra* note 20.
[25] To that end the Bitlicense rightfully includes disclosure and cybersecurity program requirements. BitLicense Proposal §§ 200.19 and 200.16.

There are two additional factors that mitigate this risk of loss. First, the user may choose only to hold and use small amounts of Virtual Currency at any time in a particular wallet or storage service. This has the added benefit of allowing the user to avoid creating records for purchases which, if aggregated or breached, could reveal embarrassing intimate details. The use of multiple wallets, then, can be both protective of privacy and security, demonstrating legitimate value in what might be perceived as identity obfuscation. Secondly, the risk of loss can be mitigated by employing security technologies native to Virtual Currency protocols, such as "multi-signature transactions" or "multi-sig."[26]

Using multi-sig, a Virtual Currency user's wallet could have three keys (hence multiple signatures) to enable use. The user could retain two of these keys—one that she memorizes or stores on her phone and another that she writes on a piece of paper and keeps in a safety deposit box—and the third key can be held by a trusted third party. This could be a loved one, or a private company dedicated to ensuring that her privately held bitcoins do not get hacked and fraudulently spent. Whenever the user's phone initiates a transaction, the third-party can sign-off so long as it doesn't look fraudulent. If the phone initiated a transfer of all of the user's funds out of her wallet to an unknown account, however, this third party could decide to not sign-off without some further contact with the user, or some good reason to believe that the phone had not been stolen. The user, meanwhile, could retain a backup key in the event that the trusted third party ever disappears and stops signing-off on *any* transactions. At this point the user could dig up her third key and move funds again, perhaps to a new multi-sig wallet with a better third-party watchdog. Multi-sig services have immense potential to protect consumers from fraud and identity theft; the Department should avoid regulatory language that could inadvertently limit their development, such as by requiring such services to keep extensive records and intrude on user privacy unnecessarily.

The privacy and security benefits of multi-sig Virtual Currency tools can be utilized without giving any custodial control of funds to third parties. In several respects, then, digital currencies are superior to the present credit card system because:

1. There are fewer intermediaries holding sensitive data;
2. Users can easily use different wallets that separate sensitive transactions from other records;
3. Users can easily initiate anti-fraud protocols that require multiple parties to sign off on a transaction without entrusting funds to those parties; and
4. As with credit cards, transactions would remain easy to initiate.

B. Mitigating Chilling Costs

With Virtual Currency, it is not necessary to have any centralized institution that associates transactional records with the user's real name and address. Some emerging digital currencies have robust privacy features intended to preserve user anonymity.[27] However, many other digital currencies, such as Bitcoin, are not entirely anonymous. Rather, they are *pseudonymous*: Each unit of Virtual Currency is associated with a particular public address—a random string of numbers and letters—and each transaction resulting in the transfer of currency from one address to another is visibly recorded on a public ledger—referred to as the

[26] *See generally* Vitalik Buterin, "Multisig: The Future of Bitcoin" *Bitcoin Magazine* (Mar. 2014) http://bitcoinmagazine.com/11108/multisig-future-bitcoin/.
[27] *See e.g.*, *ZeroCoin Project*, http://zerocoin.org/ (last accessed Oct. 16, 2014).

block chain.[28] The name or names of the people controlling that address are, however, not recorded in the block chain.

As a result, no single entity has the depth and fidelity of information regarding an individual's purchasing habits that many traditional financial institutions now possess. This feature shows great promise for mitigating chilling costs—transactions forgone for fear of public revelation. The user of a cryptocurrency can take technological steps to ensure that there is no single vulnerable database that could reveal sensitive information, such as a personal medical condition, an embarrassing but legal habit, or support for a controversial political candidate.[29]

Because the transactions are recorded publicly, a set of transactions belonging to some discrete individual or group can be observed to be benign even without knowledge or direct personal investigation of those persons. The full ledger of all transactions can be reviewed by law enforcement to flag only those transactions that appear suspicious because of their size, frequency, or interaction with known suspicious addresses. At that point, steps can be taken to de-anonymize[30] only those public addresses involved in suspicious transactions while leaving the remaining addresses and transactions private. This can help law enforcement focus limited taxpayer resources on real threats while helping to assure innocent parties that their privacy is not being needlessly violated. The Department should review ways to develop useful intelligence from publicly available block chain data.[31]

C. Mitigating Compliance Costs

Merchants and other payment intermediaries are involved in a costly effort to improve data security and fraud protection. Security technologies built on top of the existing credit card system—notably the 3-D Secure protocol[32] and chip-and-pin cards[33]—have been undergoing costly development and implementation

---

[28] Bitcoin transactions and the public addresses involved can all be viewed in real time at websites such as BlockChain.info, https://blockchain.info/.

[29] Privacy is fundamental to free speech, diversity, creativity, and democratic self-governance. *See* Neil M. Richards, "The Dangers of Surveillance," 126 Harv. L. Rev. 1934 (2013). Intuitively, we modify our behavior whenever we know or fear that we are being observed. We abstain from some activities in which we'd otherwise engage or conform to modes of acting we'd otherwise eschew. Simply put, when we are observed we become behaviorally and intellectually homogenous. This phenomena has been intuited by scholars and writers for centuries. *See e.g.*, Jeremy Bentham, *Panopticon* (1787); George Orwell, *Nineteen Eighty-Four* (1949). More recently—chilling effects have been observed empirically. *See* Alex Marthews and Catherine Tucker, "Government Surveillance and Internet Search Behavior" (August 28, 2014) *available at* SSRN: http://ssrn.com/abstract=2412564 or http://dx.doi.org/10.2139/ssrn.2412564; *See generally* Anthony Giddens, The Nation-State and Violence (1985).

[30] De-anonymizing Bitcoin transactions has proven easier than many initially expected. *See* Alex Biryukov, et al. "Deanonymisation of clients in Bitcoin P2P network," *eprint arXiv:1405.7418* (May 2014) *available at* http://arxiv.org/pdf/1405.7418v3.pdf; Elli Androulaki, et al. "Evaluating User Privacy in Bitcoin," 7859 *Financial Cryptography and Data Security Lecture Notes in Computer Science* 34 (2013); Philip Koshy, et al. An "Analysis of Anonymity in Bitcoin Using P2P Network Traffic" (Doctoral dissertation, Pennsylvania State University) (2013) *available at* http://ifca.ai/fc14/papers/fc14_submission_71.pdf; Sarah Meiklejohn, et al., A Fistful of Bitcoins: Characterizing Payments Among Men with No Names," *Proceedings of the 2013 conference on Internet measurement conference* (ACM, 2013) *available at* http://cseweb.ucsd.edu/~smeiklejohn/files/imc13.pdf.

[31] *Id.*

[32] *See* Steven J. Murdoch and Ross Anderson, "Verified by Visa and MasterCard SecureCode: or, How Not to Design Authentication", 6052 *Lecture Notes in Computer Science* 336 (Jan. 2010).

[33] *See* Brian Krebs, "The Target Breach, By the Numbers," *KrebsonSecurity* (May 6, 2014) https://krebsonsecurity.com/2014/05/the-target-breach-by-the-numbers/.

for years, but rates of fraud and identity theft rise unabated.[34] Virtual Currencies have the potential to slash these compliance costs. Because digital currencies do not necessarily require the storage of personal data on the servers of the merchant or payment intermediary, these entities can focus on providing valuable products rather than accumulating and securing a vulnerable database against hackers—an endless arms race.

Similarly, because digital currencies typically push funds from user to merchant, merchants need not be formal participants in complex payment networks designed to pull funds from—for example—a user's credit card account to the merchant. The merchant accepting Bitcoin need only receive and keep the coins or have access to a service, such as BitPay, that will rapidly and automatically exchange payment in cryptocurrency for the local fiat currency. This allows payment networks to be global and interoperable without requiring any shared global database of user account information and private financial histories, beyond a pseudonymous ledger.

II. IMPLICATIONS FOR BITLICENSE

The unique, privacy-enhancing features of digital currencies have enormous potential to reduce costs associated with identity theft and business compliance while also protecting user privacy and preserving ease of use. Many of these opportunities, however, would be significantly reduced by the Department's proposed BitLicense as proposed. Although we recognize that the Department intends for the BitLicense to protect consumers, provide business certainty, and aid law enforcement in stopping illicit transactions, the proposed BitLicense creates significant new risks and uncertainties for a wide range of Virtual Currency users. To avoid unnecessarily weakening privacy, security, and innovation in Virtual Currency services, we recommend the following adjustments to the Department's BitLicense proposal.

A. Counterparty Identification in Recordkeeping Requirements

As presently drafted, Sections 200.12(1) and 200.15(d)(1) of the proposed BitLicense require that Virtual Currency businesses (VCBs) keep records "for each transaction . . . [including the] names, account numbers, and physical addresses of the parties to the transaction."[35] This section can be interpreted to mandate the collection of information about not just the customers of an intermediary service, but also information about any third party to whom an intermediary's customer transfers funds. As a result, financial services using Virtual Currency may interpret the BitLicense to require that they record the identities and addresses of all parties for every transaction across their services.

Effectively mandating identification of counterparties would go well beyond existing recording requirements for money services businesses as found in the Financial Crimes Enforcement Network's (FinCEN's) regulations[36] under the Bank Secrecy Act (BSA),[37] the so-called "Travel Rule":

> "Before concluding any transaction with respect to which a report is required . . . a financial institution shall verify and record the name and address of the individual presenting a transaction, as

[34] *See Murdoch*, *supra* note 32. http://www.cl.cam.ac.uk/~rja14/Papers/fc10vbvsecurecode.pdf.
[35] BitLicense Proposal §§ 200.12(1) and 200.15(d)(1).
[36] *See* 31 C.F.R. §§1022.400 and 1010.312.
[37] Pub. L. No. 91-5081 (1970), codified at 12 U.S.C. §§1829b and 1951-59, and 31 U.S.C. §§ 5311-5330.

> well as record the identity, account number, and the social security or taxpayer identification number, *if any*, of any person or entity on whose behalf such transaction is to be effected."[38]

FinCEN's public guidance explicitly indicates that information about counterparties must only be recorded "*if received*,"[39] and the Federal Financial Institutions Examination Council's online manual specifies that only "[a]s many of the following [counterparty-related] items *as are received* with the payment order"[40] need be recorded. This limitation excuses financial institutions from the costly requirement of tracking down personal details for individuals that are not their own customers whenever those details are not already present in the transaction. We recognize that the Department's purposes in promulgating the BitLicense may not be coterminous with FinCEN, however we ask the Department to study FinCEN's language as an example of a carefully-drafted compromise that reflects law enforcement as well as business realities.

Breaking with the language chosen by FinCEN places a greater compliance burden on Virtual Currency companies than exists for traditional money transmitters. This could make New York an unappealing location for a Virtual Currency business, particularly if those businesses can automatically exclude online customers visiting from a New York IP address,[41] and, as an alternative to seeking a BitLicense, comply with a different state's ordinary money transmission requirements and the BSA.[42]

Nor is this heightened requirement a trivial addition; compliance would be costly and disruptive. Mirroring FinCEN's requirements is particularly reasonable given that the per-transaction recordkeeping demanded by FinCEN only applies to transmittal of funds in the amount of $3,000 or more[43] while the Department's applies "without limitation."[44] Financial intermediaries of virtual currencies should not be forced to spend resources tracking and describing each chewing gum vending machine or Hebrew National food cart that their customer happens to use.

New York would also be requiring businesses to surveil their customers and take on greater data-security risks, by mandating the construction of vulnerable databases replete with full transaction histories and other private information. As explained earlier, the privacy and efficiency benefits of cryptocurrencies are contingent on maintaining the possibility that counterparties will be strangers to the transaction initiator. A cash user does not need to know the name or physical address of the corner deli clerk in order to give him

---

[38] 31 C.F.R. § 1010.312.

[39] Financial Crimes Enforcement Network, "Funds Travel Regulations: Questions & Answers," 7 *FinCEN Advisory* 3 (Jan. 1997) (emphases in original), *available at* http://www.fincen.gov/news_room/rp/advisory/pdf/advissu7.pdf.

[40] Federal Financial Institutions Examination Council, *Funds Transfers Recordkeeping—Overview*, https://www.ffiec.gov/bsa_aml_infobase/pages_manual/OLM_025.htm (last accessed Oct. 16, 2014) (emphases in original).

[41] Software engineers can design websites that block all incoming visitors from certain geographic locations. This is achieved by filtering traffic based on the visitor's IP address, a number that is broadcast by all networked computers and mobile devices. Lists exist that indicate which IP addresses originate from which regions. For example, a list has been made of all IP addresses in and near Nigeria, in an overbroad effort to stop spam and scam emails, which frequently originate from users in that country. *See* Wizcrafts Computer Services, *Block Nigerian Scammers From Apache Based Servers or Forums with a .htaccess Blocklist*, http://www.wizcrafts.net/nigerian-blocklist.html (last accessed Oct. 16, 2014).

[42] For example, the State of Texas, which will regulate virtual currency exchanges as money transmitters but avoid any additional or divergent requirements. Aman Batheja, "Texas Banking Chief Issues Rules for Bitcoin," *Texas Tribune* (April 11, 2014). https://www.texastribune.org/2014/04/11/texas-banking-chief-issues-rules-bitcoin/.

[43] 31 C.F.R. §1010.410.

[44] BitLicense Proposal § 200.12(a).

four dollars for a sandwich. Building a system so that the user would always know the name and address of her counterparty would only repeat the vulnerabilities of the existing credit card payment scheme: a suite of intermediaries that hold and share sensitive data, each of which is a target for hackers.

Creating a central repository of identity and transaction information may recreate the data liabilities of traditional payment systems. As demonstrated through the Target data breach, extending the network of parties to private information enhances the risk of identity theft.[45] Keeping detailed records of counterparty data may just as easily enable criminals as it would stymie them. Similarly, such a repository could chill legitimate but embarrassing or private uses of cryptocurrencies, because it could be used to build a robust and intimate catalog of all the personal transactions of any Virtual Currency user.

Decentralized digital currencies, such as Bitcoin, natively lack such centralized repositories.[46] It is unclear where such a repository would exist, if mandated by law, or who would be tasked with building it, maintaining it, and securing it against malicious hackers. Payment processors building services on top of the Bitcoin protocol, for example, already have this information for their own customers in order to comply with existing licensing and "know-your-customer" (KYC) requirements, but these businesses will not be able to, either by contractual demand or technological process, consistently obtain it from those with whom they are not in privity.

The Department has clearly expressed its intent to tailor the BitLicense to the "unique characteristics" of Virtual Currencies.[47] Requiring the development of a non-trivial technological addition (recipient identification databases) and eliminating key pro-consumer features (payment without data retention) would be antithetical to that tailoring.

RECOMMENDATION: The Department should adjust the recordkeeping requirements so as to avoid mandating counterparty identification. It should mirror the language in federal recordkeeping law, *e.g.* FinCEN's codified regulations under the Bank Secrecy Act. Section 200.12(a)(1) should be adjusted to read as follows:

> "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, the names, account numbers, and physical addresses of the initiator of the transaction, and the names, account numbers, and physical addresses, ***if any are provided with the transaction order***, of any person or entity on whose behalf such transaction is to be affected."

Section 200.15 (d)(1), an identical passage related to the mandated "Anti-money laundering program" should also be adjusted in the same fashion.

B. Exclude individual uses from "Virtual Currency Business Activity"

The proposed definition of Virtual Currency Business Activity (VCBA) at § 200.2(n)(1) should not be defined to include individual uses of Virtual Currency when unmediated by firms. As presently drafted,

---

[45] *See infra* at p. 4.

[46] While the block chain publically lists all transactions to and from pseudonymous addresses, it does not list personal details.

[47] *See* New York State Department of Financial Services, *Notice of Intent to Hold Hearing on Virtual Currencies, Including Potential NY-DFS Issuance of a 'BitLicense'* (Notice, Nov. 14, 2013), http://www.dfs.ny.gov/about/press2013/virtual-currency-131114.pdf.

VCBA includes "receiving Virtual Currency for transmission or transmitting the same," and "storing [or holding] Virtual Currency on behalf of others."[48] This may apply intrusive customer identification requirements to personal transactions and services controlled entirely by the user. We doubt this was the intention of the Department,[49] but the language of the proposed BitLicense does not make that clear. As applied to individual uses of Virtual Currency, the proposed BitLicense is unnecessarily detrimental to user privacy, prohibitive of common sense Virtual Currency products, and raises constitutional issues.

For example, as currently drafted, the BitLicense would apply intrusive customer identification and transaction tracking requirements to every type of Virtual Currency wallet. Wallets are crucial to users of Virtual Currency since the currency (or, more accurately, the credentials that indicate the user's ownership of the currency) must reside somewhere.[50] Wallets are software and can be designed and built by a sophisticated Virtual Currency user (in a DIY fashion) or by a third party intermediary service, and can store Virtual Currency credentials in the cloud or locally on a personal device, such as a smartphone.[51] Even if a wallet is created solely by the user and not on behalf of others, and stores the Virtual Currency credentials locally on a personal device, the user could be subject to the regulations if her wallet "transmits" the Virtual Currency to another person.[52] In general, users should not be required to provide identifying information and submit to transaction tracking to use software tools that are unmediated by firms with custody or control of the Virtual Currency.

Another example: as currently drafted, the proposed BitLicense includes a limited exemption from licensing requirements for merchants and consumers using Virtual Currency for the purchase or sale of goods or services.[53] However, this would not cover many person-to-person or non-merchant transactions—such as gifts, charitable or political contributions, a friend paying a debt, etc.—thereby imposing the BitLicense's intrusive recordkeeping requirements on users engaged in financial activities that can often be particularly private,[54] or even—under some circumstances—merit legally protected anonymity under the First Amendment.[55]

In addition, the proposed BitLicense's application to individual uses of Virtual Currency raises potential Fourth Amendment constitutional issues. The Supreme Court has found it constitutional for the government to require banks to create records about their customers,[56] which the government may then seize or search,

---

[48] BitLicense Proposal § 200.2(n)(1).

[49] *See* 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 (explaining that "[t]he new DFS BitLicenses will be required for firms engaged in . . . Receiving or transmitting virtual currency *on behalf of consumers*[.]") (emphases added).

[50] *See generally* "Wallet," *Bitcoin Wiki*, https://en.bitcoin.it/wiki/Wallet.

[51] *Id.*

[52] BitLicense Proposal § 200.2(n)(1).

[53] BitLicense Proposal § 200.3(c)(2).

[54] *See* Jerry Brito and Eli Dourado, *Comments to the New York Department of Financial Services on the Proposed Virtual Currency Regulatory Framework* (Mercatus, Aug. 2014) *available at* http://mercatus.org/publication/comments-new-york-department-financial-services-proposed-virtual-currency-regulatory.

[55] *See* NAACP v. Alabama ex rel. Patterson, 357 U.S. 449 (1958) (finding that "compelled disclosure, in itself, can seriously infringe on privacy of association and belief guaranteed by the First Amendment.").

[56] The Court, in *California Bankers Assn. v Shultz*, found that no reasonable expectation of privacy had been breached when banks were required to collect and store customer records. The Court reasoned that a bank was a "party to any negotiable instrument drawn upon it by a depositor, and upon acceptance or payment of an instrument [the bank] incurs

reasoning that those customers have no expectation of privacy in records voluntarily provided to the third party banks.[57] However, an individual using Virtual Currency under their own control is not necessarily entrusting any personal data to a business or third-party, thereby preserving the individual's reasonable expectation of privacy in any non-public data[58] related to their own, unmediated use of a Virtual Currency network.[59] These individuals may therefore have standing to assert Fourth Amendment rights over their personal Virtual Currency records, should they even be in the habit of keeping them. This potentially conflicts with the BitLicense's requirement, at § 200.12(b), that licensees provide the Department with access to search VCBA-related records upon request.[60]

RECOMMENDATION: We recommend that the definition[61] of VCBA be modified as follows:

> "receiving Virtual Currency for transmission or transmitting the same"

should be tailored to explicitly apply *only* to transmission by intermediary services with custody of Virtual Currency, excluding user-controlled software:

> "receiving ***custody*** of Virtual Currency for transmission, or transmitting the same, ***on behalf of others***."

Since releasing the proposed regulations, Superintendent Lawsky has indicated that licensure should not be required of individual Virtual Currency users.[62] We applaud this clarification and hope the Department utilizes the above language to formalize that distinction. If, however, recordkeeping requirements are to be imposed on individual use of digital currency in any form, the requirements should focus only on transactions that involve high dollar amounts, high volume, or high risk parties or goods.[63]

---

obligations to the payee." California Bankers Assn. v. Shultz, 416 U.S. 21, 48. Given that the bank was therefore a party to the transactions—rather than a "conscripted neutral[] in transactions"—the Court reasoned that mandated record collection was not a form of government surveillance, i.e. not a scenario where banks were serving solely as agents of the state. Shultz, 416 U.S. at 52-3 .

[57] The Court, in United States v Miller found that "[a]ll of the documents obtained, including financial statements and deposit slips, contain only information voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business." United States v. Miller, 425 U.S. 435 (1976). Accordingly, the court held that depositors had no fourth amendment interest in records held by banks because those records contained information revealed to a third party. Entrusting private data to a third party thus destroys an individual's reasonable expectation of privacy and denies the individual standing to challenge a search. *Id.* at

[58] This would not, of course, include any data that the user places on the publicly visible block chain.

[59] *Under Katz v. United States*, law enforcement must comply with the "procedure of antecedent justification," i.e. obtain—generally—a search warrant, before searching or seizing the private papers of a citizen. The *Katz* court reasoned that the Fourth Amendment protects people not places and therefore protects intangibles—e.g. records—as well as physical property. See Katz v. United States 389 U.S. 347 (1967).

[60] BitLicense Proposal § 200.12(b).

[61] BitLicense Proposal § 200.2(n).

[62] Benjamin Lawsky, New York State Superintendent of Financial Services, Keynote Address at Benjamin N. Cardozo School of Law Event: Regulating Digital Currency: BitLicense and the Internet of Value" (Tuesday, October 14, 2014) *available at* http://cardozolaw.hosted.panopto.com/Panopto/Pages/Embed.aspx?id=01b5be00-c8df-4688-a1dc-5302b6ca3c7e&v=1&internal=true&autoplay=true

[63] FinCEN, for example, already has reporting requirements for overseas movements of ten thousand dollars or more. *See e.g.*, Dept. of Treasury, *Form 105 Report of International Transportation of Currency or Monetary Instruments*, (Mar. 2011), http://www.fincen.gov/forms/files/fin105_cmir.pdf.

C. Exclude Ancillary Services and Services that do not Have Full Custodial Control

The proposed definition of VCBA at § 200.2(n)(1) encompasses services that "secure" or "transmit" Virtual Currency "on behalf of others."[64] This broad language could impose onerous and intrusive recordkeeping requirements on services that are incidental to Virtual Currency transactions. For example, could "secure on behalf of others" mean that cybersecurity or antivirus software vendors must identify Virtual Currency users whom they protect? Could "transmit" encompass Internet service providers, like Comcast or Time Warner, whose networks transport Virtual Currency credentials? The BitLicense proposal is unclear.

Without custodial control of the user's Virtual Currency, a service need not be entrusted with the individual's sensitive records. The records they would be forced to obtain under the BitLicense would be in no way natural or relevant to their business activities.[65] Placing these complex recordkeeping requirements on security services would be highly detrimental both to financial privacy generally and to New York as a hub for financial security innovation. Additionally, these requirements may—as with individual recordkeeping and reporting—be unconstitutional.[66]

Services that do not have full custodial control of a user's Virtual Currency should not be required to collect user identity and transaction information. For example, as described earlier, services that maintain a single key to a multi-sig wallet do not have custodial control over the wallet funds. Instead these services provide a valuable monitoring and fraud-protection role[67] that would otherwise be unavailable to cryptocurrency users. The ability to have such fraud protection without the liabilities inherent in granting full custodial control of sensitive personal financial information to an intermediary, such as a credit card company, is one of the most promising cybersecurity innovations within Virtual Currency.

RECOMMENDATION: To avoid a multitude of potentially outlandish interpretations, we recommend reworking § 200.2(n)(2) so that it reads:

> "~~securing, storing, holding, or~~ maintaining ***full*** custody or control of Virtual Currency on behalf of others;"

---

[64] BitLicense Proposal § 200.2(n)(1).

[65] *Cf.* Shultz, 416 U.S. at 52-3 ("The fact that a large number of banks voluntarily kept records of this sort before they were required to do so by regulation is an indication that the records were thought useful to the bank in the conduct of its own business . . .").

[66] Without custodial control, the intermediary neither needs nor desires to be entrusted with the individual's sensitive records. As per the Court in *Schultz*, the intermediary—in the unique case of cryptocurrency—is nothing more than a "conscripted neutral[] in transactions." Shultz, 416 U.S. at 48. Therefore, requiring recordkeeping from cryptocurrency intermediaries that do not have custody of coins or a natural interest in the recorded data is tantamount to making these entities act, as per *Miller*, "solely as agents of the Government." Miller, 425 U.S. at 443. The *Miller* opinion includes dicta that even this sort of government mandate may be constitutional. *See id.* This possibility is not explored by the Court and only two cases are offered as support: Osborn v. United States,385 U. S. 323 (1966), and Lewis v. United States,385 U. S. 206 (1966). Both of these cases involve the use of listening devices attached to willing government informants. It seems dubious to suppose that widespread recording of private financial data could be constitutional purely because these cryptocurrency intermediaries agreed to become government informants.

[67] *See e.g.*, *BitGo*, https://www.bitgo.com/ (last accessed Oct. 15, 2014).

For custodial accounts accessible to or controlled by third parties holding funds or credentials on behalf of users, we recommend that BitLicense should be no more intrusive or onerous than current federal requirements for money transmitters.[68]

In addition, the Department should widen its exception for online gaming currencies. The proposed BitLicense includes an exception—at § 200.2(m)—for online video game currency, but only if the currency has no market outside of the gaming platform. Yet currencies for most major online games are often sold in online marketplaces for fiat money. For example, Eve Online's Intersteller Kredit is readily available from unauthorized sellers,[69] at least one exchange openly trades Second Life Linden Dollars for Bitcoin,[70] and rare gaming items are often for sale on online auction sites.[71] Given the external markets for such gaming currencies and artifacts, it would seem many gaming companies—as issuers of Virtual Currency—may not be protected by the proposed regulations' exception for video game currency. External market activities are generally not authorized by the gaming company,[72] but New York's proposed regulations do not make that distinction. To avoid requiring the gaming companies to record the identities and transactions of users of their currencies, we recommend that the BitLicense encompass only those online gaming currencies with company-authorized marketplaces outside of the game.

D. Exclude Decentralized Virtual Currencies and Issuance

The BitLicense places identical regulatory requirements on two fundamentally different types of Virtual Currency: centralized and decentralized. A centralized Virtual Currency is under the singular control of a firm or organization; this entity has plenary authority to issue new currency, recognize or fail to recognize Virtual Currency transfers, and control all currency in the ecosystem. Placing trust in these currencies means placing trust in the single institution tasked with administering it. This trust can be abused, resulting in fraud and crime.[73] The Department has rightly chosen to regulate organizations that opaquely develop and administer their own centralized Virtual Currencies.[74]

However, decentralized Virtual Currencies, have proven less attractive to criminals. Edward Lowery, Special Agent for the United States Secret Service, testified before the Senate Committee on Homeland Security and Governmental Affairs Committee that "within what we see in our investigations, the online cybercriminals, the high-level international cybercriminals we are talking about, have not, by and large, gravitated towards

---

[68] 31 C.F.R. 1022.

[69] *See, e.g., IskMarket* http://iskmarket.com/ (last accessed Oct. 15, 2014).

[70] *See VirWoX FAQ*, https://www.virwox.com/faq.php?stage=2 (last accessed Oct. 15, 2014).

[71] *See, e.g., Ebay listing for "Diablo 3 | Wand of Woh - WoH,"* http://www.ebay.com/itm/Diablo-3-Wand-of-Woh-WoH-Available-on-EU-US-SC-HC-Limited-Spots-/181489028877?pt=UK_PC_Video_Games_Video_Games_JS&hash=item2a4196cf0d (last accessed Oct. 15, 2014).

[72] *See, e.g., IskMarket FAQ*, http://iskmarket.com/en/FAQ#faq_146 (last accessed Oct. 15, 2014).

[73] *See, e.g.*, Indictment of Arthur Budovsky, U.S. v. Liberty Reserve et al. *available at* http://www.justice.gov/usao/nys/pressreleases/September14/MaximChukharevPleaPR/Liberty%20Reserve,%20et%20al.%20Indictment%20-%20Redacted.pdf.

[74] BitLicense Proposal §200.2(n)(5).

the peer-to-peer crypto-currencies such as Bitcoin."[75] Decentralized currencies are also less prone to fraud and manipulation because no single entity holds the power to manipulate the technology to their benefit.[76]

Truly decentralized currencies have two distinguishing characteristics. First, the protocol on which they run—all of the software that allows users to issue, administer and interact with the currency—is open-source.[77] That means every detail that makes the currency run from a technical standpoint can be viewed and assessed by anyone without seeking permission. Second, the actual processing of transactions is performed by an open peer-to-peer network. Individuals that wish to become involved with processing, referred to as as mining, are free to join that network by connecting and dedicating their computing power, and the pseudonymous ledger of these transactions is distributed and made publically visible.[78] Given these built-in protections from fraud and manipulation, the Department should adjust its treatment of decentralized Virtual Currencies in the Bitlicense.

First, a clear distinction between centralized and decentralized digital currencies should be made.[79] Using the two distinguishing features of decentralized Virtual Currency, we propose the following definition, to be included in 200.2(m) or in a new standalone definition:

> Decentralized Virtual Currencies are digital units of value that are issued and transferred without a central administrative authority, using an open network that runs transparent, non-proprietary software, and that shares resources among network participants.

Second, decentralized Virtual Currencies should not be regulated at the level of issuance, control, or administration. Open groups of individuals volunteer their time to maintain and develop computer code that is then voluntarily adopted by the user-ecosystem to power the network. Users of the currency lend their own computing power to maintain that ecosystem, under the expectation of probabilistic rewards.[80] Accordingly, issuance and administration activities are already entirely transparent; there is no obscured information to be demanded by regulators, nor is there a central entity from which to demand such information—or any entity that could leverage it for illegal purposes. Given that these currencies are open-source and transparent by design, regulatory and compliance efforts should not be expended duplicating the publication of available information regarding administration and issuance.

RECOMMENDATION: The definition of "Virtual Currency Business Activity" at § 200.2(n)(5) should read:

---

[75] Lowery Testimony, *supra* note 85 (quote comes from question and answer session and was not, therefore in written testimony submitted by Lowery).

[76] *See* Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, pp. 6-8, *available at* https://bitcoin.org/bitcoin.pdf.

[77] The full source code of Bitcoin, for example, can be found in the software repository site Github, here: https://github.com/bitcoin/bitcoin.

[78] The ledger is referred to as the Blockchain, and can be explored in full using free tools on websites such as https://blockchain.info/.

[79] The BitLicense already contemplates this distinction at § 200.2(m) of the proposal. The distinction could be improved, however, to more clearly differentiate between centralized currencies, which pose real risks of manipulation or fraud, and decentralized currencies, which because of their transparency have in-built protections against such manipulation.

[80] This is what is referred to as mining. *See generally* "Mining," *Bitcoin Wiki* (last accessed Oct. 15, 2014) https://en.bitcoin.it/wiki/Mining.

(5) controlling, administering, or issuing any Virtual Currency ***that is not decentralized***

The continued flourishing of decentralized, open, and transparently administered currencies serves the Department's interest in protecting New Yorkers from crime and fraud. Limiting the development of these innovations, as compared with centralized currencies, may not serve the Department's mission or the public at large.

E. Transaction Obfuscation

Many virtual currencies, including Bitcoin as presently implemented, 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.[81] Although pseudonymous, this address information can potentially be traced back to the individual, revealing the individual's financial and transaction history.[82]

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.[83] Traditional payment methods generally require large, fixed minimum processing fees. This makes their use for very small payments uneconomical. 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.[84] 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.) 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.[85] 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

---

[81] 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/.

[82] *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.).

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

[84] *See* Visa, *Visa U.S.A. Interchange Reimbursement Fees* (Apr. 2014), http://usa.visa.com/download/merchants/Visa-Interchange-Reimbursement-Fees-April-2014.pdf

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

that Virtual Currency users be permitted to obfuscate transactions so that they are not—as would be the Virtual Currency 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 block chain, 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.

RECOMMENDATION:

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 the section be construed to make illegal 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."

Finally, the best source for improving any lurking financial privacy liabilities within cryptocurrencies will likely be continued innovation and development, including the development of entirely new alternative cryptographic currencies. The software on which Bitcoin runs is open source and can easily be downloaded, modified, and shared to create new, potentially improved cryptocurrencies.[86] The Department must not foreclose the development of these new and potentially improved decentralized Virtual Currencies by requiring costly registration and recordkeeping. To that end, as discussed earlier, decentralized currencies should not be regulated at the level of issuance or administration.[87]

F. Suspicious Activity Reports

The BitLicense creates a new, state-level Suspicious Activity Reports (SARs) obligation[88] in addition to existing federal requirements from FinCEN.[89] Unlike FinCEN's language, the BitLicense has no lower bound on what size transactions merit reporting.[90] Merely duplicating SARs already required by federal law and sending them to the Department as well as FinCEN may not be an onerous burden on VCBs. However, compliance costs would be likely to increase if the standards for SARs vary between the federal and the state level, particularly if there is no state minimum for when SARs are not required.

---

[86] *See, e.g.*, *LiteCoin* https://github.com/litecoin-project/litecoin, and *DogeCoin* https://github.com/dogecoin/dogecoin, both of which have been "forked" (that is to say, copied, modified, and re-released) from the original Bitcoin software repository at https://github.com/bitcoin/bitcoin.
[87] *See infra* at pp. 13-15.
[88] BitLicense Proposal § 200.15.
[89] 31 C.F.R. § 1022.320.
[90] BitLicense Proposal § 200.15.

SARs should not be required in cases where the activities observed by the Virtual Currency business do not rise to the requisite level for scrutiny under federal law. Without a lower limit on what might constitute reportable suspicious activities, risk-averse Virtual Currency businesses may simply report any and all activities even when these activities involve trivial amounts. The resulting deluge of personal information transferred to the Department via SARs could harm the financial privacy of legitimate users while creating an administrative nightmare for regulators tasked with collecting and filtering through these many reports.

Accordingly, the federal standard should apply: 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.[91] The Department should revise its SARs requirements under § 200.15 to match, and not exceed, Federal requirements.

Conclusion

Privacy and robust consumer protection are essential to a flourishing financial services industry. Bitcoin and other emerging virtual currencies represent the first meaningful opportunity to improve on a payment system that's grown insecure, unwieldy, and inefficient—all to the detriment of consumers as well as law enforcement. The Department is to be commended for its forward-facing goal: tailoring financial regulations to the unique qualities of such promising technologies. If the recommended modifications described above are adopted by the Department, New York will, indeed, pave the way for safer, faster currencies, as well as the wellspring of innovation and commerce that may follow.

[91] 31 C.F.R. § 1022.320(a)(2).