



February 16, 2015

Attn: Emerging Payments Task Force
Conference of State Bank Supervisors
1129 20th Street NW, 9th Floor
Washington, D.C. 20036

Re: Draft Model Regulatory Framework
and Request for Public Comment

Ladies and Gentlemen:

Xapo, Inc. (“*Xapo*”) respectfully submits the following comments on the Draft Model Regulatory Framework (the “*Draft Framework*”) proposed by the Conference of State Bank Supervisors (“*CSBS*”). We appreciate the efforts undertaken by the CSBS in crafting a framework to implement its policy on state regulation of virtual currencies, which involve novel technologies and applications that are evolving quickly, in ways and with implications that cannot currently be anticipated. We believe that the Draft Framework is a well-thought starting point for the discussion, and our specific responses to the questions for public comment are set forth below. Please note that, as Xapo offers a hosted bitcoin wallet and vault for consumers and enterprises, our discussion of virtual currencies is limited to bitcoin.

1. Policy Implementation – Entities engaged in virtual currency activities might not be engaged in traditional money transmitter activities involving only fiat, government backed currencies. Similarly, traditional money transmitters might not be engaged in virtual currency activities.

a. Within the umbrella of state money transmitter regimes, how can state regulators appropriately tailor licensing and supervision to each set of licensees?

We believe that existing money transmitter licensing frameworks are the proper starting point for regulation. These frameworks are well-established and well-defined, offering predictability and clarity. In addition, these frameworks are well understood by legal and accounting service providers, making it easier for companies in the nascent bitcoin industry to seek counsel in a cost- and time-effective manner. This expertise and accumulated experience provide a known path to bitcoin companies wishing to comply with regulatory requirements. However, as the question suggests, many bitcoin companies may be engaging in activities that are not squarely addressed by or otherwise contemplated by the existing frameworks. We believe it is important to enable flexibility in the system, to regulate based on volume and activity, and to design an implementation period for attaining compliance.

Flexibility. Bitcoin transactions by their nature rely on a decentralized technology that is not present in traditional financial services. This technology is rapidly evolving and has applications that cannot yet be anticipated or even understood. As such, the rapidity of this change may require a more flexible approach to allow for the underlying technology to reach its full potential. We believe that regulation should consider this rapid pace of technological development, which is not present in the conventional financial services businesses that existing frameworks are designed to address.

Volume and Activity. Bitcoin transactions may be at a level so small as to not be suitable for existing regulation, or possibly any regulation at all. As such, we believe it is appropriate to include safe harbors or carve-outs for transactions (whether individually or in aggregated value) that, by their nature, do not require regulatory oversight. Bitcoins are divisible to 8 decimal places, and if necessary, the bitcoin technology can be modified to enable greater divisibility. This allows for bitcoins to be used for micro-transactions that are otherwise currently prohibitive (for example, “tipping” less than a penny worth of bitcoins to a blogger for a good post). In many of these micro-transaction cases, existing regulation may not make sense at all, as the cost of compliance will outweigh the ability to provide services to user, which may have the untended effect of forcing consumers to use less reputable services.

Implementation Periods. Any regulations should include an onboarding period during which bitcoin companies can bring their operations into compliance. Many companies in the bitcoin industry are start-ups, with limited access to engineering and development resources. Products, services, and processes that are not aligned with final regulations will require a grace period in which to bring these businesses into compliance. Further, such regulations should consider the size of the entity to be regulated and balance regulatory goals while fostering the nascent bitcoin technological ecosystem. A safe harbor for smaller companies would be helpful in achieving this goal.

b. In order to properly tailor licensing and regulatory regimes to virtual currency activities, should states consider a virtual currency-specific “amendment” or “endorsement” to a traditional money transmitter license?

Yes, states should consider the amendment/endorsement process. This could provide flexibility to states, allowing them to eliminate requirements that may be inapplicable or to augment existing frameworks with new requirements that are not otherwise contemplated. For example, unlike traditional financial services transactions, each bitcoin transaction is non-reversible once it has been verified by the bitcoin network and recorded in the public blockchain ledger. This means that there is no mechanism for the reversal of a transaction. This is a critically important element of a bitcoin transaction, allowing for both a sender and receiver to transact without fear of repudiation. However, this means that where a transaction was processed in error or in an erroneous amount, or initiated as a result of fraud, there can be no recourse through the bitcoin network. As such, requirements around repudiation may need to be tailored or modified.

Further, bitcoin transactions are transparent but pseudo-anonymous. This means that all bitcoin transactions can be viewed in the public blockchain ledger, however, they are not otherwise tied to a party that is personally identifiable. Some services, such as Xapo, require users to verify their identities are part of accessing a fully-feature bitcoin wallet through our service. But unlike conventional financial services, the information gathering and sharing requirements for bitcoin companies will differ significantly from conventional financial services companies.

Our understanding is that many existing state money transmitter licensing frameworks may not be extendable to bitcoin companies in the absence of legislative processes that could be time consuming to implement. As this could inhibit regulators from providing short-term clarity on the rules of engagement and longer-term flexibility to enhance and improve regulation with technology changes, we believe an amendment/endorsement process could be very useful.

2. Licensing Process

a. Though states largely have the same licensing requirements, there is not a common implementation process. Please comment on the functionality of the NMLS or other licensing systems.

We believe that a common application and implementation process would be highly valuable, not only for digital currencies, but for any business seeking money transmitter licenses. The process of applying for licenses is extraordinarily expensive, requiring significant in-house time and expertise and often demanding very costly third party legal advice.

Bitcoin (and virtual currency generally) is decentralized by its nature and is available to customers throughout the United States and internationally, irrespective of the location of a company’s headquarters. This means that bitcoin companies must pursue a multi-state licensing strategy, which can be daunting at best, and prohibitively costly at worst (whether in terms of time, money, or employee resources). As a result, even the most compliance-oriented companies might choose to operate without a license, believing that the short-term costs of doing so outweigh the long-term penalties for failure to comply. We favor a framework that allows such companies to meet their compliance obligations efficiently and cost-effectively.

Xapo has utilized the NMLS system, and we believe that the implementation of the system by all states would be an important step in reducing the costs and increasing the efficiency associated with applying for multiple licenses. It would also be beneficial to expand the scope of data submitted through NMLS, such as the credentialing data discussed in the other answers to this Question 2.

b. Would a common application and guide to licensure enhance the efficiency of the licensing system?

Yes, a common application and guide for licensure would greatly enhance the efficiency. Bitcoin companies typically have consumers throughout the U.S. from the outset and are required to repeat the application processes in different states without a harmonized framework and without a common application system, which is expensive and time-consuming.

c. Obtaining required criminal background checks has been flagged as an administrative challenge in the licensing process. What procedures can states uniformly adopt to facilitate obtaining criminal background checks as part of the licensing process?

While we believe that the requirement for any specific element (criminal background check, fingerprints, etc.) should be left to the discretion of the state, the cost and time associated with obtaining these elements is high. A background check procedure that is harmonized among all states would be very beneficial to companies. A procedure specifying common elements to be verified (for example, felony and misdemeanor convictions in all counties lived in the past 10 years) and the process by which these can be verified (for example, by a third party or self-disclosure by an applicant) would allow companies to provide responsive information in a streamlined and efficient manner.

d. Credentialing business entity key personnel can be a hands-on process, but has proved indispensable for financial services licensing. Are there alternative means of credentialing that may facilitate the process?

The existing credentialing process would be far less burdensome if harmonized among all states. As with the background checks, a common set of data and procedure that could be utilized to comply with all states would be very helpful. Bitcoin companies will typically have users spread throughout the United States, requiring licensure in multiple jurisdictions. So while the credentialing process can be time consuming, particularly as it requires the time of those tasked with running the business rather than tending to administrative tasks, we strongly believe that the greater challenge is posed by the time and expense needed to repeat this process over and over again for each state. We favor a process in which credentials can be obtained once and securely shared multiple times.

3. Training and Education – Educating regulators about virtual currency business activities and business models is an important part of building a responsive and robust regulatory structure.

a. What education may be necessary for state regulators to aid in the licensing process?

We believe that a general understanding of bitcoin's underlying technology is helpful, though not necessary. The internet offers an illustrative example. Regulators don't need to understand the internet's data transmission protocols at the technical level to understand how people use the internet (often through personal experience) and to craft rules designed to protect consumers, deter fraud, and provide other benefits.

There are many useful sources of information on bitcoin and the bitcoin industry. Xapo has met with various federal, state and international regulatory agencies, and would be pleased to assist with any education efforts (as are many other bitcoin companies). We also believe that simply opening a bitcoin wallet, which is a straightforward process, could be a helpful way for regulators to learn more. Much like opening an email account or an on-line bank account, the initial technological and information requirements are minimal.

b. What resources are available to explain technology and business models across the virtual currency industry?

Xapo and many of the other top bitcoin companies are valuable resources for training and education. Xapo maintains a blog at blog.xapo.com with relevant articles and background materials, including a YouTube video titled "Bitcoin and the History of Money" at <http://youtu.be/IP0jCjyrew8>. A partial list of other useful sources of information include the Bitcoin Foundation, research and advocacy groups like Coin Center, consulting firms like Promontory Financial Group and Coin Comply, and bitcoin news outlets like CoinDesk and CoinTelegraph. In addition, industry organizations such as ACAMS and CFCS provide compliance-specific training.

4. Technological Innovations – What changes and innovations have been seen and/or can be anticipated in the technological aspects of virtual currencies and the resulting marketplace?

The bitcoin technology is extremely new. The technology underlying bitcoin was made public fewer than seven years ago, and most companies in the industry have operating histories of only a few years. As such, we anticipate numerous and varied changes and innovations in the heavily technology-dependent bitcoin industry. There have already been significant changes in the technologies bitcoin companies are using to increase security. Multi-signature authorizations and deterministic wallets are two innovations that provide for greatly enhanced security for users, reducing the risk of exposure to errors by users and to fraud or other malfeasance by any one bitcoin service provider. As we contemplate future improvements, we believe that an implementation period for any regulation as well as a safe harbor for smaller companies, as discussed in the answer to Question 1.a, would be critical.

5. Denomination of Capital, Permissible Investments, and Bond Coverage – Capital, permissible investments, and surety bond requirements exist to create financial security in the event of failed transactions or a failed business. For financial services companies dealing in virtual currencies, should these safety funds be denominated in the applicable virtual currency or in dollars?

We believe that bitcoin companies should have the flexibility to determine whether these safety funds are denominated in bitcoins or dollars based on their business model and on the type of transactions against which risk is being hedged. For many businesses, the obligation owed to customers is in bitcoins (for example, selling bitcoins to a consumer requires settling that transaction in bitcoins), and many companies may need to hold large balances in bitcoin. For other businesses, the obligation may only be settled in dollars (for example, buying bitcoins from a consumer requires settling that transaction in dollars). For custodians of bitcoin, operating much like a traditional safety deposit box, other considerations may apply and holding dollar-denominated balances may not apply. The Draft Framework seems to anticipate flexibility as to the amounts that would be required to satisfy safety fund obligations based on activities and volume, and we believe it would be appropriate to extend this flexibility to denomination of the funds. In deciding the relative level of flexibility, the numerous business models employed by bitcoin companies should be taken into account.

6. Distressed or Failed Companies – Certain requirements in the Draft Framework are designed to provide regulators with tools for dealing with distressed or failed companies. Please comment on the practical issues and challenges facing regulators in the case of a distressed or failed company. What other tools should regulators have for resolving a failed virtual currency company, minimizing consumer harm and market impact?

We believe that regulators should consider tools to prevent and to deter failures. For example, ongoing monitoring, through periodic reporting, would allow an opportunity for deficiencies to be addressed in advance. In addition, we believe that deterrents, in the form of penalties associated with failures caused by fraud or illicit activity will be important in aligning the behavior of management teams in advance of a failure event.

7. Consumer Protections – What consumer remedies should policy makers consider for virtual currency financial activities and transactions?

Clear consumer disclosures should be a first step in protecting consumers. Given the decentralized nature of bitcoin, the volatility of the market, and the irreversibility of bitcoin transactions, (and the lack of an established fee structure to compensate bitcoin service providers, as with credit card interchange fees), consumers should be provided with notice of these risks. We believe that clear notice of these risks in a company's terms of use should be a minimum requirement. Model provisions for use by compliance-oriented companies with limited resources for expensive outside advisors could be formulated and would be helpful.

At this stage, careful consideration should be made where consumer remedies include recourse to a service provider to compensate for the risks described above. We believe that the bitcoin ecosystem is enhanced by the presence of third party service providers, who are able to build far more secure architectures than individuals can create on their own. However, third party service providers are not a requirement for the ecosystem, and consumers can engage in bitcoin transactions on their own (as individuals), facing reduced security. If a liability layer is attached to third party service providers for inherent risks in the system, particularly as there are no established fee

structures to compensate for the increased risk, many service providers may reasonably decide to not participate in the ecosystem, with the unintended effect of reducing consumer protection.

8. State Insurance or Trust Funds – Some states have laws that create a trust or insurance fund for the benefit of instrument holders (i.e., holders of checks, money orders, drafts, etc.) in the event that a licensed money transmitter defaults on its obligation or is otherwise unable to make payment on the instrument. Is it appropriate to allow holders of instruments denominated in virtual currency access to such insurance or trust funds?

Given the irreversibility of bitcoin transactions and the nearly instantaneous ability to publicly confirm transactions in the blockchain ledger, we believe the risk of default on bitcoin transactions is reduced as compared to conventional financial services providers. However, where bitcoin service providers are taking orders in dollars that are subject to later fulfillment in bitcoin, we think it would be appropriate to extend to users such consumer protections as are afforded to users of conventional financial instruments.

9. BSA/AML – Fraud and illicit activities monitoring are increasingly technology based and proprietary, especially for virtually currency companies. Are state and federal exam procedures current with regards to new methods of detecting BSA/AML activity?

While the technology underlying the bitcoin protocol and utilized by bitcoin service providers is nascent, the credit and debit transactions (and typologies for illicit activities and fraud) associated with the ecosystem are similar to those found in conventional financial services transactions, and largely implicate the same regulatory oversights. For example, the three stages of money laundering (placement, layering, and integration) are as applicable in the bitcoin ecosystem as they are within any payment system (thought at a much lower volume, given the lower volume of the currency available). As such, the current regulatory expectations and exam procedures, such as the FFIEC exam manual, seem adequate to detect and address BSA/AML activities in the bitcoin industry. In addition, as with existing money transmitter frameworks, these exam procedures are well-established, providing consistency and predictability to compliance-oriented bitcoin companies. A harmonized reporting system, including through the use of regulatory reporting application programming interfaces, or APIs, would also enhance the efficiency of the compliance process.

10. Customer Identification – The Draft Framework includes maintaining records on the identification of virtual currency owners. Credentialing consumers for identification purposes can be accomplished to varying degrees, from basic account information to verified personal identification. What is the appropriate level of identification?

We believe that for hosted bitcoin wallets, such as those offered by Xapo, consumers should be required to provide a basic minimum level of information to create an account and use it up to nominal dollar thresholds. In part due to the micro-transactions that are possible with bitcoin, it's possible for anyone with a smartphone to have a bitcoin account and for such account to hold the equivalent of less than a penny of value. We think that for users to understand the technology and realize its benefits, it's imperative that users have an opportunity to use bitcoins with a nominal dollar amount without completing as rigorous of an identification procedure as with a conventional financial bank account. But we believe that verified personal information must be provided in order for such a user to use a hosted bitcoin wallet for transacting or saving above nominal sums.

11. Regulatory Flexibility – The Draft Framework stresses regulatory flexibility to accommodate different activity levels and business models and to avoid inhibiting innovation.

a. Given the rapidly evolving nature of virtual currencies, what should be the nature of any necessary flexibility?

We believe that clear regulatory guidance is critically important to allowing bitcoin companies to start to manage their businesses more consistently. We believe that existing money transmitter licensing frameworks in many states can offer a clear starting point. However, the technologies underlying all virtual currencies offer potential benefits (and risks) that cannot be fully understood today. Bitcoin companies are like conventional money services businesses in many respects, but certain technological aspects of bitcoin mean that some exceptions or alternatives may become necessary as the technology grows and develops. As discussed above, we believe that providing safe harbors and carve-outs for transactions that may not require regulatory oversight would be important.

b. How can laws and regulations be written to strike a balance between setting clear rules of the road and providing regulatory flexibility?

We think that New York's BitLicense Proposal attempts to strike a balance by establishing rules but affording discretion to the superintendent in certain cases. The risk is that this type of discretion can create unpredictability, may be inconsistently applied, and may even be subject to abuse (for example, favoring one business model or company over others). We believe that a framework that accommodates certainty of regulatory rules and intent where possible is optimal. We recognize that flexibility is necessary and believe that such flexibility should be coupled with a procedure for the issuance of "no action" letters. Such a procedure would allow the system to maintain flexibility, all the while providing a formal communication channel in which novel innovations can be explored in a legally compliant fashion, reducing regulatory and legal risk for businesses. This is the practice of the Securities and Exchange Commission and the Internal Revenue Service and has been recently proposed by the Consumer Financial Protection Bureau.

12. Reporting Requirements – Most states require money transmitter licensees to submit periodic reports of business activities.

a. For licensed virtual currency companies, what types of information and data should be included in periodic reports?

Examples of appropriate data elements could include changes in financial and business condition (including changes in executive management), and aggregated transaction values and volume from dollars into bitcoin (and bitcoin into dollars) per state. As a general matter, we believe that the types of information and data that should be reported periodically should be standardized among states. The ideal case would be that a single standardized report could be completed and used to comply with periodic reporting requirements. As with the credentialing requirements discussed in the answers to Question 2, the issue is less with the specific information requested and more the burden of complying with myriad different requirements.

b. What technology solutions exist to mitigate regulatory reporting requirements?

Many existing technology solutions are unavailable for companies to meeting reporting requirements. Many commercially available technology solutions are designed for mature enterprises, and are not scaled for small companies, which poses challenges to the bitcoin industry. This means that third party services are often too costly or too complex to integrate in order to provide meaningful benefits. Further, many of these providers have not adapted their offerings to service bitcoin companies, though several have indicated an intention to do so. As a result, many companies must develop their own proprietary systems. The burden of this process could be reduced by harmonizing reporting requirements among states and by allowing for submissions through the use of reporting application programming interfaces, or APIs.

13. Technological Solutions to Improve Supervision – State exams and reporting requirements reflect an institution at a point in time. Conversely, operational standards and internal compliance audits increasingly offer the opportunity for real time data collection, interacting with transmission data to ensure adequate funding, anti-money laundering compliance, fraud protection, and consumer protection. What technology solutions can regulators and licensees deploy to close information gaps in a manner that makes the supervisory process more efficient and "real time?"

We do not believe that the supervisor processes of regulators should be "real time" in the sense of overseeing a business on an ongoing basis. This would require the creation of unwieldy compliance apparatuses in each company that isn't consistent with a developing industry. Conventional banking reporting is also not required to be in real time as many such reporting events require further investigation or must be conducted thoughtfully in order to achieve regulatory goals. Further, bitcoin companies often cannot use the third party technologies that could otherwise reduce the complexity of meeting reporting obligations. Consequently, many are responsible for developing their own technology solutions. We believe that bitcoin companies should be required to maintain documented policies to ensure that systems and controls are in place to monitor transactions for fraud, consumer protection and AML, and these should be subject to at least periodic self-audit and audit by a qualified third party auditor depending on volume and activities.

14. Cyber Risk Insurance. Companies have begun looking to insurance to help manage cyber risks, and there are a growing number of companies offering cyber liability insurance. What role should cyber risk insurance have in a licensed virtual currency entity's approach to managing cyber risks? Please discuss the potential costs and benefits for virtual currency companies securing cyber risk insurance.

We believe that cyber risk insurance should be recommended by not required and that consumer disclosure of the applicability (or inapplicability) of insurance should be made available. We also believe that bitcoin companies should be held to industry standard technology measures to protect user data and the underlying bitcoins themselves. An example would be multi-signature authorizations, which are quickly being adopted by the top companies to safeguard data. Each company should be required to maintain documented security policies and procedures, and these should be subject to at least periodic self-audit and audit by a qualified third party security auditor depending on volume and activities to ensure compliance therewith. But we believe that insuring against other data risks should be left to the reasonable business judgment of each company.

These policies are, for the most part, considerably more expensive for bitcoin companies than for non-bitcoin financial services and technology companies, in part due to a lower understanding of the risks posed. For instance, there is also a meaningful distinction between insuring so-called "hot" bitcoin wallets and "cold" bitcoin storage. Hot bitcoin wallets are connected to the internet and can face a meaningful cyber risk (whether through hacking, corporate negligence, employee theft, user error, or otherwise). Cold bitcoin storage is never connected to the internet, and carries limited, or no, cyber risk. Xapo has incorporated a captive insurance company to offer a primary level of insurance to its vault customers, and built out a co-surety group on top of this with four well-known A and A++ A.M. Best rated companies (which we are unable to name publicly, though the information is available to our customers in a logged in section of their account). Due to the cost of the program, Xapo and other industry counterparts, would not have been able to obtain insurance had they not been well capitalized.

So while we support securing a cyber risk insurance policy for our business, making it a requirement could stifle innovation by smaller companies, who simply could not afford the cost. We also believe there may be opportunities for bitcoin companies to reduce risk through technological innovation (as with multi-signature authorizations) or to pool their risks to get more advantageous pricing, but this should be driven by business concerns rather than by regulatory requirements.

15. Commercial Fund Transfer Liability – Article 4A of the Uniform Commercial Code establishes liability for wire transfers, relying on definitions strictly applicable to banks. Are provisions like those in Article 4A necessary for commercial transfers denominated in virtual currencies? If so, is the Article 4A construct an appropriate model to be adapted in a manner that is not bank-centric?

Bitcoin transactions are non-reversible once they have been verified and recorded in the blockchain ledger. There is no mechanism for the reversal of such a transaction if it was initiated in error or through fraudulent means. Further, bitcoin transactions are "push" transactions in that they can only be initiated by a user and not requested by a third party (for example, a bitcoin user can only send bitcoins to a specific email or blockchain address, rather than a third party being able to request withdrawal). As such, we do not believe that provisions like those in Article 4A are appropriate or capable of adaptation for bitcoin transactions.

16. Banking Services for Virtual Currency Companies – Banking arrangement information is necessary for evaluating the safety and soundness of a licensee. However, virtual currency businesses are not immediately understood by most banks that provide traditional money services accounts. What are the risks facing banks that consider banking virtual currency companies, and how can those risks be mitigated?

One of the deepest operational challenges facing bitcoin companies is the difficulty in obtaining bank accounts, including for simple day-to-day purposes not related to bitcoin (such as paying employees and vendors). The ability to obtain bank accounts for transactional purposes (such as buying or selling bitcoins for customers) is nearly impossible. This is a function of the fact that only a handful of banks have been willing to learn more about bitcoin businesses.

We believe that the issue is not that banks face greater business risks in working with bitcoin companies (other than the risks common to a banking relationship with any money services business). Rather, that the

regulatory environment is so unclear as to make it unmanageable for many of these banks to engage meaningfully with bitcoin businesses. The banks currently working with bitcoin banks face enhanced scrutiny from regulators, which requires additional staff, deeper expertise, and greater expense. We are grateful for our relationships with these few banks, but it has an unintended consequence of concentrating operational liability in the space. Fewer banks supporting bitcoin businesses subjects the eco-system to higher concentration risk and decreased bargaining power. We believe that a regulatory framework that provides clear guidelines will be beneficial for bitcoin businesses, because it will enable the third parties on whom they depend to have greater clarity in assessing the risks they face.

17. *Merchant-Acquirer Activities – Companies processing credit card payments between a buyer’s bank and a seller’s bank (Merchant-Acquirers) have historically been presumably exempt from money services businesses statutes because of their nexus to the highly regulated banking system. A company processing virtual currency payments for merchants who accept virtual currency as payment for goods and/or services may exchange virtual currency to dollars, which can then be transferred to the merchant’s bank account. Is this activity akin to the activities of traditional Merchant-Acquirers, or is it the exchange and subsequent transmission of value that is typically regulated by the states?*

Xapo does not currently engage in these type of transactions, and we do not have a comment at this time.

18. *Cost – State regulators are cognizant of the costs associated with licensure and ongoing compliance. What processes can be implemented to reduce these costs, including any shared services or technology-based reporting?*

State licensure and compliance obligations require an investment of considerable amounts of money and employee time, which in smaller companies with limited staffing may be even more burdensome. The use of common filing and reporting systems would be immensely helpful in reducing costs. The ability to complete an application once and securely share it multiple times would help companies in applying for required licenses and taking the necessary steps to comply with reporting obligations. The actual cost of licensure can also be overly burdensome. Given the nascent nature of the industry with regulatory obligations still evolving, a lower rate for licensure applications would allow companies with shorter operating histories to still comply with legal and regulatory requirements.

19. *Escheatment – How should virtual currency be treated under state escheatment laws?*

We believe that virtual currency should be treated in a like manner to other unclaimed property (that is, generally subject to escheatment to the state following notice to the consumer and with a process for consumer recovery from the state thereafter). However, it would be important to accommodate technological limitations that may not apply to conventional unclaimed property. For example, a bitcoin company may not be able to remit funds to its respective state given the implementation of multi-signature security protocols (which allow users to hold private keys needed to authenticate transfers and other transactions).

* * * *

We are grateful for the opportunity to respond to the request for public comment, and we look forward to continuing to engage with CSBS to reach an appropriate and balanced set of regulations.

Very truly yours,



Cindy McAdam
President and General Counsel