January 14th 2017

From:
Ubixi Inc.
Fremont, CA
info@ubixi.com
510 468 6385

To:
Illinois Department of Financial & Professional Regulation
100 W. Randolph St., Floor 9 Chicago, Illinois, 60601-3218

To whom it may concern at the IDFPR:

We thank you for inviting comments on the ‘Digital Currency Regulatory Guidance’. The document is comprehensive on the views of centralized versus decentralized currencies. We also understand that the Transfer of Money Act (‘TOMA’) referenced in the document addresses only decentralized currencies.

While Ubixi would not be considered a ‘Money Transmitter’ per the definition in your document, we thought it was important to share our views and expertise in this area, especially as it relates to digital assets and the regulatory framework. Ubixi is a technology startup that is building payment solutions for capital markets. More specifically, Ubixi’s platform enables members to achieve on-demand clearing and settlement of assets, and the execution of complex workflows such as Delivery Versus Payments, Free of Payment, or Collateral versus Cash.

Prior to Ubixi, the leadership team at Ubixi has worked in both banks and traditional electronic payments companies and have implemented BSA/AML and OFAC for new payments systems. More specifically, to comply with the Patriot Act, we have executed KYC for individuals and businesses. We have also instituted CIP and SAR reports for new electronic payments that work primarily using the Internet. We highlight these backgrounds as we think they are very relevant to the comments we seek to provide to the document.

In this response, we would like to refer to a few prior publications and reports by regulatory bodies.

- Financial Crimes Enforcement Network: FinCEN March 18, 2013: report (details in reference 4) referred to as FinCEN report in this document.

- Federal Reserve Bank of Atlanta: Banking Bitcoin (details in reference 4) Related Businesses. A primer for managing BSA/AML Risks referred to as Fed Atlanta Report in this document

- Conference of State Bank Supervisors (CSBS): The State of State Money Services Businesses Regulation and supervision. (details in reference 5) referred to as CSBS report in this document

We will base our comments broadly into the following sections.

1. State of innovation in digital currencies and timing for regulation
2. Mapping of MTRA (Money Transmitters Regulators Association) framework to digital currencies
3. Recommendation on a phased approach

1. State of innovation in digital currencies and timing for regulation:

The world of digital currencies has seen a wide range of innovation. We have seen more complete product offering and market choices in the following:

- Investments, innovations, consortiums and open source communities for shared ledgers, digital identities, and proof-of-concepts in capital markets solutions
- Increased number of transactions and higher acceptance of digital currency by businesses
- Capital Market Trades, investment vehicles such as mutual funds in digital currencies and futures for digital currencies
- Digital Currency Wallets

We also want to highlight some of the challenges the industry is facing:

1. Increased theft from the sources of money that are held in digital wallets
2. Lack of understanding of the regulatory framework
3. Some inconsistency between regulatory bodies on the approach

Considering this, we believe it is the right time to start putting into place the framework of regulation. Proper regulation helps set up the rules of the road and helps protect the customers and businesses. Proper guidelines and execution for onboarding, reporting, auditing, enforcements and training helps all participants in the long run. In this regard, we welcome the state's action to seek comments for digital currency guidance. In the CSBS document referenced above, it states that a proper regulation and enforcement framework for MSBs and Money Transmitters will reduce the 'indiscriminate de-risking resulting in the elimination of MSB accounts". We agree with this statement and think proper regulation should help bring these businesses and money flows through them, become more mainstream.

We also want to highlight that while regulation is important, inconsistent guidelines between regulatory bodies adds confusion to the industry. This is particularly true when the ecosystem that we are attempting to regulate is rapidly evolving and is likely to look very different in three to five years. While this may seem like rapid progress, we believe it is still very early days for mainstream adoption of digital currencies. We refer to the Bank of England consultation paper in the references section.

Because the ecosystem is in the early days, in the next section, we compare the current regulatory reporting and enforcement framework for Money Transmitters in traditional and electronic banking to the digital currency ecosystem.

2. <u>Mapping of MTRA (Money Transmitters' Regulators Association) framework to digital currencies</u>

We refer to the CSBS report which lists the various modules in the regulatory framework (pages 6 to 13) . We will then compare them to the framework of digital currencies in an effort to highlight some areas where the current framework may not be optimal. The recommendations will follow this gap analysis:

1. Credentialing
2. Supervision
3. Coordinated Enforcement between Federal and State agencies

2a. Credentialing:

This refers primarily to the onboarding and licensing requirements, as well as the background checks of the owners. The important items to focus on are the following:

1. Ensuring MSBs and MTs are qualified to do business
2. Ongoing accountability to the public
3. Prevention of MSBs and MT as a conduit to do business for illicit activities

The Uniform Money Services Act is used as the statutory provision by many states. This is a robust framework that has evolved over several years. The dynamics of traditional money movement especially for AML activities (placements, layering and integration) have been well understood. Therefore, the credentialing can ensure that licenses are issued to the right businesses and that they are better prepared to protect public money and act within the legal framework.

We want to point out that the dynamics of money movement is different for digital currencies. The primary differences that we want to point out are the following:

(a) Pseudo Anonymous Nature of the transactions: A BitCoin address is a public key of a public/private key pair. It is very difficult to find the private keys and therefore difficult to find the real-world owner. (Please see reference item 2 in this document.)

(b) Origination and termination of fund flows may be outside the preview of the money transmitters and MSBs: While most bitcoin activities are legitimate, we will use one specific example to highlight a general problem with the ecosystem. Businesses and individual users are now seeing an increase in ransomware. This can be done with malware or a threat of a DOS/DDOS attack. Fraudsters behind the ransomware, use BitCoin as the prefered payout. This type of a funds flow may appear legit for the systems because of the pseudo anonymous nature. KYC is weak in the world of digital currency and it is relatively easy for fraudsters to mask these as legitimate transactions originating from different keys and IP addresses.

(c) Absence of ‘bank’ for auditability purposes: The digital wallet is the closest analogy to a ‘bank’ (with some major differences) in the digital world as it acts as the depository or custodian of the funds. We have seen an increased number of high profile attacks on digital wallet providers. In addition, identity takeovers in the world of digital currency is a serious issue as safekeeping of private keys is not understood in depth by ‘users’ of digital currency. We also acknowledge the innovation in the world of digital wallets in the last two years. However, the anonymous nature of the digital currency world makes it harder to bring comparable levels of fraud prevention and auditability to the digital world.

2b. Supervision:

BSA/AML is a substantial portion of the supervision for money transmission. Here, we refer to the CSBS report on page 10 and the Fed Atlanta paper (pages 6 to 9). The reporting requirements for BSA/AML fall into the following categories:

a. Currency Transaction Reports (CTRs)
b. Suspicious Activity Reports (SARs)
c. Foreign Banks and Foreign Account Reports (FBARs)

AML consists of three main steps (a) Placement (b) Layering and (c) Integration. The Fed Atlanta paper specifically addresses the issues for these when dealing with Digital Currency where it is relatively easy for a launderer to perform these actions without triggering alerts or revealing the identity. The pseudo anonymous nature of the currency makes it harder. The paper also talks of some of the innovations that some of the wallet providers are undertaking. This is a first step that will need enhancements over the years.

2c. Coordinated Enforcement between Federal and State Agencies:

This is a critical part of successful enforcement. However, we wish to point out that consistency of a framework between the different regulatory bodies is necessary for this. While the state has attempted to keep the definitions of a money transmitter as close to the FinCEN, we think some of the language in the state’s paper such as ‘Generally Qualifying as Money Transmitters’, carve out of ATMs that are configured in a specific way and can lead to inconsistent interpretation by officials. We want to refer to the Fed Atlanta’s paper which has summarized the FinCEN’s definitions well (page 11). We request that the state also either adopt this or come up with a well-defined table such as this.

Inconsistencies and interpretations make it difficult for startups and midsize companies to seek and achieve full compliance. Further, it can lead to enforcements that can be harsh or even fatal for young companies. This will only drive innovation out of the state or even the country. We want to point out only a very small percentage of the bitcoin mining is currently being performed in the United States.

3. Recommendations of a Phased Approach

We have emphasized that the digital currency ecosystem is new and evolving, and that the regulatory and supervisory framework that exists for traditional money transmission needs to be adjusted to fit with the new ecosystem. Our recommendations are the following:

a. Framework for security and adequate identity management: We believe it is important for regulatory bodies to take a lead position and establish some security frameworks. Ubixi has been working with the Federal Reserve and a other regulatory organizations. We understand the depth and breadth of expertise in security at these organizations. Unless a company is primarily in the business of security, it will be hard for them to be as comprehensive in the understanding or expertise in security.

b. KYC: With the understanding of the pseudo anonymous nature of the ecosystem as well as the emerging innovations, we believe it is important to define what constitutes adequate knowledge of a customer within the digital currency world .

c. Review of what is considered suspicious activity (SARs): We realize that publishing this will set the boundaries for launderers to work just outside this ring-fence. However, we think some indicators such as velocity checks or grouping based on IP are examples of features that could be useful. In addition, during the placement and integration phase of laundering, grouping the bank accounts could help identify suspicious activities.

d. CTRs and FBARs reports also need to be adapted to the new ecosystem. We have some suggestions we can share if there is interest.

e. Safeguards to the Digital Wallets world: As one of the objectives of regulation is to protect people's money, we think better safeguards around wallets can improve the ecosystem. We believe the regulators should work closely with the wallet companies to define standards for protection

f. Everyday, US Citizens and Residents face ransomware threats: While we realize that the regulators are not responsible for tracking and bringing these fraudsters to justice, we think it is important to closely monitor the ecosystem. As previously mentioned, this system is continuously evolving and enforcement activities should do all they can to keep abreast of the changes.

g. Continuous training in online security practices: We think the AML certification process should be augmented to handle security and identity in the digital currency world.

References

1. Bank of England's request for comments on the RTGS consultation paper (http://www.bankofengland.co.uk/markets/Documents/paymentsystem/cp160916.pdf) where the power of digital currency was acknowledged. However, the bank took the stance that digital currency and distributed ledger technologies were not mature enough to the point for integration into the RTGS system. The Bank has made this decision after a very detailed study and direct interaction and participation in several projects involving digital currency and distributed ledgers.

2. https://blockchain.info/ is a website that monitors the latest activity in the bitcoin blockchain. Clicking on links show the depth of the chain and specific details about transactions and the associated hashes

3. Financial Crimes Enforcement Network: FinCEN March 18, 2013: (https://www.fincen.gov/sites/default/files/shared/FIN-2013-G001.pdf) . FinCEN has also provided a few clarifications on it original report on the various categorizations

4. Federal Reserve Bank of Atlanta: Banking Bitcoin – Related Businesses. A primer for managing BSA/AML Risks (https://www.frbatlanta.org/-/media/documents/rprf/rprf_pubs/2016/banking-bitcoin-related-businesses.pdf)

5. Conference of State Bank Supervisors (CSBS): The State of State Money Services Businesses Regulation and supervision. (https://www.csbs.org/regulatory/Cooperative-Agreements/Documents/State%20of%20State%20MSB%20Regulation%20and%20Supervision%202.pdf)