LAW360 Tax Authority
a LexisNexis® company

Portfolio Media. Inc. | 111 West 19th Street, 5th floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Ohio's Risky Foray Into Bitcoin: Part 2

By **John Reed Stark** (December 13, 2018, 10:13 AM EST)

John Reed Stark

Cryptocurrency enthusiasts are celebrating. Ohio has created a system where its taxpayers can tender their tax payments in bitcoin, boldly going where no U.S. state has gone before. But this is not good news and is actually quite worrisome.

Ohio ironically hopes to portray itself as a crypto pioneer and an epicenter of innovation, but its bitcoin gamble, whether well-intentioned or political ploy, is a disaster waiting to happen.

This two-part series discusses why Ohio's treasury, or any other state or federal government entity, should be the very last institutions to even consider accepting this dubious form of payment.

Part one of this series provided some background concerning bitcoin and then continued with a discussion of the liquidity, fraud, price volatility and manipulation risks associated with Ohio's crypto adventure. Part one also incorporated a discussion of Ohio's bitcoin collection process, including the participation of BitPay, the financial intermediary Ohio has engaged to execute the tax payment transactions, but that is not registered as an Ohio money transmitter business.

Part two now: (1) tackles the array of intricate money laundering issues pertaining to Ohio's crypto efforts together with other concerns for the state, such as cybersecurity risk, tax hazards and Office of Foreign Assets Control implications; and (2) provides some final thoughts and suggestions going forward.

Money Laundering Risks

The Financial Crimes Enforcement Network's anti-money laundering requirements, combined with state law money services business licensing and bonding requirements (such as Ohio's money transmitter licensure requirement), not only create a hefty, burdensome and onerous federal and state regulatory burden and concern, they also enhance the risk significantly for the state of Ohio and for crypto intermediaries like BitPay.

Theoretically, anyone with an internet connection and a digital wallet can own bitcoin — which, of course, opens the door for those with criminal motives. Given that cryptocurrency transactions are pseudonymous, encrypted and decentralized by nature, virtual currencies offer a convenient method of transferring funds obtained from illegal activities without an audit trail, thereby making it harder for any central authority or law enforcement agency to track each of the transactions made, and to identify the individuals behind any of them.

On the other hand, transactions involving traditional financial firms, such as banks, brokers and dealers, and money service businesses, are subject to strict U.S. anti-money laundering laws and regulations aimed at detecting and reporting suspicious activity, including money laundering and terrorist financing, as well as securities fraud and market manipulation.

Along these lines, the New York State Attorney General's Office asked 14 popular crypto trading platforms to respond to a detailed questionnaire covering a wide range of topics, from trading fees to anti-money laundering policies to methods for keeping customer assets secure. Ten chose to comply, and the September 2018 report of their responses illuminates the shadowy inner workings of cryptocurrency trading platforms, raising serious questions regarding the growing

workings of cryptocurrency trading platforms, raising serious questions regarding the growing connection between cryptocurrency and money laundering — as well as a range of market manipulation concerns.

Not surprisingly, the notion of terrorists and criminals being able to launder money anonymously has not escaped the attention of U.S. law enforcement agencies, which have vowed to crack down on the cryptocurrency warehousing and conversion firms that serve criminals, even those operating outside the United States. The U.S. Department of Justice, acting in cooperation with FinCEN, has become increasingly active in policing criminals exploiting cryptocurrencies, leveraging AML statutes and regulations as the preferred statutory prosecutorial weapon.

For instance, as far back as 2015, in addition to being charged for conspiracy to commit bank fraud and conspiracy to obstruct an examination of a financial institution, Anthony Murgio, the son of a Palm Beach County school board member and bitcoin exchange operator, also pled guilty to operating as a money transmitter without a license, and was sentenced to 5 ½ years in prison. Federal prosecutors alleged Murgio and his co-conspirators benefited from transactions providing victims with bitcoin to pay off ransomware demands. The indictment states:

> As part of the unlawful Coin.mx scheme, Anthony P. Murgio, the defendant, and his co-conspirators knowingly processed and profited from numerous Bitcoin transactions conducted on behalf of victims of ransomware schemes ... By knowingly permitting ransomware victims to exchange currency for Bitcoins through Coin.mx, Murgio and his co-conspirators facilitated the transfer of ransom proceeds to the malware operators while generating revenue for Coin.mx.

Not just a part of the ransomware payment process, Murgio allegedly facilitated the ransomware transactions with unclean hands — possessing the kind of nefarious intent required for money laundering criminal liability, which is probably why the Murgio prosecution also addresses AML liability. Specifically, the issues relate to the failure of Murgio and his cohorts to:

- Register with FinCEN;
- Maintain an effective AML program;
- Comply with AML record-keeping requirements; and
- File with FinCEN suspicious activity reports regarding customers who use cryptocurrencies for nefarious purposes.

The Murgio indictment also alleges that Murgio and another defendant had undue influence on a federally insured credit union that handled the trading platform’s banking operations for a period of time, and that they tried to “trick” major financial institutions about the nature of their business. The Murgio defendants allegedly exchanged at least $1.8 million bitcoins for cash for certain customers who claimed they were ransomware attack victims needing bitcoins to "pay off" ransomware attackers.

FinCEN, MSBs and Cryptocurrency

MSBs have been required to register with FinCEN since 1999, when the MSB regulations first went into effect. An entity acting as an MSB that fails to register (by filing a registration of money services business, or RMSB, and renewing the registration every two years per 31 U.S.C. § 5330 and 31 C.F.R. § 1022.380), is subject to civil money penalties and possible criminal prosecution.

MSBs have historically been recognized by FinCEN to include: (1) currency dealers or exchangers;

(2) check cashers; (3) issuers of traveler’s checks, money orders or stored value; (4) sellers or redeemers of traveler’s checks, money orders or stored value; and (5) money transmitters.

There is no cost for FinCEN registration, which is a simple procedure explained in detail on FinCEN's website — and BitPay has filed this simple form. However, acceptance of a FinCEN MSB filing is not a recommendation, certification of legitimacy, or endorsement of the MSB registrant by FinCEN or any other government agency. The registration of the MSB merely serves as a first step in establishing the compliance framework for applicable FinCEN regulations designed to help mitigate the risks of criminal abuse of MSBs for money laundering and terrorist financing as the

MSB seeks to provide financial services to customers for legitimate purposes.

The Bank Secrecy Act and its implementing regulations require an MSB to develop, implement and maintain an effective written AML program that is reasonably designed to prevent the MSB from being used to facilitate money laundering and the financing of terrorist activities. For entities like BitPay, this would require, among other things, meticulously recording transactions, definitively knowing who customers are, and reporting suspicious activity to law enforcement. Is BitPay conforming to these requirements? Tough to tell because MSB regulation is state-based — with each state promulgating its own priorities and requirements ranging from record-keeping and bonding to audits and reporting.

For instance, a cryptocurrency firm could be subject to onsite audit and scrutiny of individual transaction activity for AML compliance, which in turn could lead to institutional and management civil liability, penalties, fines, license revocation — even potential criminal exposure for individuals caught intentionally circumventing AML obligations.

Indeed, in January 2018, New York State Financial Services Superintendent Maria T. Vullo announced that Western Union agreed to pay a $60 million fine as part of a consent order with the DFS for violations of New York Bank Secrecy Act and AML regulations. An investigation by DFS found that Western Union failed to implement and maintain an anti-money laundering compliance program to deter, detect and report on criminals' use of its electronic network to facilitate fraud, money laundering and the illegal structuring of transactions below amounts that would trigger regulatory reporting requirements.

Vullo stated at the time:

> Western Union executives put profits ahead of the company's responsibilities to detect and prevent money laundering and fraud, by choosing to maintain relationships with and failing to discipline obviously suspect, but highly profitable, agents. DFS will not tolerate unlawful activity that undermines anti-money laundering laws and endangers the integrity of our financial system.

Watch **this video** to hear Vullo's take on bitcoin; it becomes clear that New York state, by taking on the mammoth regulatory responsibility of overseeing all things crypto in its territory, may have bitten off way more than it can chew.

FinCEN's MSB Expansion

Recently, FinCEN has begun to expand its definition of an MSB even further, to include not only virtual currency trading platforms but also cryptocurrency platforms that act as enablers or financial intermediaries for criminal schemes.

For instance, in a July 2017 AML enforcement action, FinCEN, in a joint prosecution by the U.S. Attorney's Office for the Northern District of California, assessed a $110 million civil money penalty against BTC-e, aka Canton Business Corp., for willfully violating U.S. AML laws. Russian national Alexander Vinnik, one of the operators of BTC-e, was also arrested in Greece, and FinCEN assessed a $12 million penalty against him for his role in the violations.

BTC-e is an internet-based, foreign-located money transmitter that exchanges fiat currency as well as the convertible virtual currencies bitcoin, Litecoin, Namecoin, Novacoin, Peercoin, Ethereum and Dash. By volume, BTC-e is one of the largest virtual currency trading platforms in the world. As such, the trading platform facilitated numerous transactions connected to a variety of criminal activities ranging from illegal drug sales on dark web markets like Alpha Bay to public corruption.

FinCEN asserted jurisdiction because BTC-e conducts business as an MSB in substantial part within the United States (including $296 million of U.S. customer transactions through U.S servers.) The BTC-e FinCEN action marks just the second case by FinCEN involving a cryptocurrency trading platform and the first FinCEN action against a foreign-based trading platform that did substantial business in the United States.

In announcing the AML fines and prosecutions, Jamal El-Hindi, then acting director for FinCEN

In announcing the AML fines and prosecutions, Jamal El-Hindi, then acting director for FinCEN, stated:

> We will hold accountable foreign-located money transmitters, including virtual currency exchangers, that do business in the United States when they willfully violate U.S. anti-money laundering law. This action should be a strong deterrent to anyone who thinks that they can facilitate ransomware, dark net drug sales, or conduct other illicit activity using encrypted virtual currency. Treasury's FinCEN team and our law enforcement partners will work with foreign counterparts across the globe to appropriately oversee virtual currency exchangers and administrators who attempt to subvert U.S. law and avoid complying with U.S. AML safeguards.

Ohio officials should carefully review FinCEN's guidance on the Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies and obtain compliance advice and counsel when necessary. If BitPay conducts business with shady characters, their actions could nonetheless raise AML red flags by facilitating such transactions.

Clearly, the noxious mix of AML and MSB federal and state regulatory requirements not only creates a foggy, deadly compliance labyrinth for cryptocurrency firms — but is also replete with risk for anyone (or any U.S. state) doing business with them.

Cryptocurrency OFAC Concerns: A Matter of Life and Death

Aside from a deep due diligence process of a crypto-paying taxpayer, Ohio and BitPay might also have to conduct other verification processes for offshore taxpayers, such as those required by the U.S. Treasury's Office of Foreign Assets Control. Ohio published a list of the 23 types of taxes for which Ohio will accept bitcoin, ranging from petroleum activity taxes to international fuel agreement taxes — surely some offshore entity will fall into one or more of these categories.

Every U.S. person and business is required to avoid engaging in financial transactions with certain individuals, entities and countries that are subject to U.S. economic sanctions. Accordingly, if Ohio's collection of bitcoin triggers OFAC compliance, it is Ohio's and BitPay's obligation to ensure that none of its business taxpayers are on the list of prohibited individuals or entities maintained by OFAC. Ohio and BitPay might also need to be sure that Ohio taxpayers are not based in countries subject to broader economic sanctions.

For its part, OFAC recently released guidance, issued in the form of frequently asked questions. The FAQs explain that transactions involving cryptocurrencies will be treated the same as other transactions — a position that multiple Treasury Department officials have signaled for several months.

In addition, in late November, OFAC took the significant step of adding digital currency addresses to its list of identifiers for certain designated individuals, stating that similar to traditional identifiers, "these digital currency addresses should assist those in the compliance and digital currency communities in identifying transactions and funds that must be blocked and investigating any connections to these addresses." Over 7,000 transactions in bitcoin, worth millions of U.S. dollars, have processed through these two addresses — some of which involved SamSam ransomware-derived bitcoin.

This was announced as part of the Treasury Department's joint action with the DOJ, in which charges were filed against an alleged Iranian hacking enterprise involved in a ransomware scheme, where two Iran-based individuals "helped exchange digital currency (bitcoin) ransom payments into Iranian rial on behalf of Iranian malicious cyber actors involved with the SamSam ransomware scheme that targeted over 200 known victims.

The Treasury Department identified the two alphanumerical wallet addresses utilized by the defendants and included them on the list of identifiers for designated individuals. With this listing, any person or business that engages in transactions with these two addresses "could be subject to secondary sanctions." The decision to include digital currency wallet addresses on OFAC's specially designated nationals and blocked persons list not only alerts those entities that transact in digital assets and incentivize them to take appropriate action but also sounds the alarm about the dangers of these kinds of transactions.

Compliance with the economic sanctions programs administered by OFAC and compliance with the AML laws established under the BSA are often considered in the same breath. However, while effective OFAC screening and AML programs will certainly have areas of overlap, namely a robust customer identification procedure, they are two separate and distinct programs and responsibilities, requiring separate and distinct procedures for each.

With respect to OFAC and AML considerations, it is also important to recognize and appreciate that cryptocurrency is a global phenomenon. This makes identifying the source of cryptocurrency, or in the least, confirming that the cryptocurrency is not somehow tainted by unlawful conduct, especially challenging, if not impossible. Like accepting a $50,000 roll of $100 bills, the cash's very existence raises questions pertaining to its purity. Moreover, merely because a $50,000 roll of $100 bills does not have blood stains on it does not alleviate the obvious suspicion about its origin.

Tax Liability Implications

Ironically, Ohio's tax payment plans could also trigger additional tax liability aggravation for its participants. Payment of taxes in cryptocurrency creates an interesting problem: If a taxpayer has purchased bitcoin some time ago and has an unrealized gain, discharging a liability such as an Ohio tax obligation, with such an appreciated asset, will lead to a taxation of the gain. In other words, payment of taxes in bitcoin may trigger more taxes — or perhaps even an IRS inquiry into the origin of that bitcoin payment.

An Ohio tax payment in bitcoin could also provide a useful road map for the IRS, which could investigate the bitcoin payment and audit the taxpayer on the tax liability. The IRS engaged in a similar investigation in late 2017 involving Coinbase related to the transactions of over 14,000 users. Coinbase was America's largest platform exchanging bitcoin with U.S. dollars by the end of 2015, claiming to have served 5.9 million customers and exchanged $6 billion in bitcoin through its buy/sell trading functionality. The IRS served a "John Doe" summons on Coinbase seeking information from a wide range of records and documents regarding U.S. persons conducting convertible virtual currency transactions at any time from 2013 through 2015.

Coinbase refused to comply, which resulted in an IRS enforcement action, and a U.S. federal magistrate judge ordered Coinbase to turn over the relevant records, ruling that virtual currency holders were clearly not outside the IRS' reach. To read the judge's order, click **here**.

Ohio's taxpayers will need to insure proper accounting for any bitcoin capital gains, while the state of Ohio should warn its taxpayers that they cannot avoid any state or federal taxation of any bitcoin gain merely because the taxpayer made the bitcoin payment to satisfy a tax bill.

Cybersecurity Risks

By registering and interacting with any cryptocurrency institution, Ohio is inviting not just possible identity theft but also exposing its operations to a potential cyberattack. Unlike Fed-insured banks and U.S. Securities and Exchange Commission registered broker-dealers and investment advisers, cryptocurrency platforms and operators like BitPay might not abide by a rigorous regime of cybersecurity rules and requirements, and may lack not only appropriate cybersecurity practices, policies and procedures, but also skilled data security personnel and hardened cyber infrastructure. This creates vulnerabilities not just to external threats but threats from their own internal employees, customers, contractors and operators.

Looking Ahead

The odd popularity of bitcoin, with its anti-establishment and libertarian appeal, has grown almost exponentially over the past few years, achieving cultural icon status, even appearing within the plots of a range of popular television shows.

For instance, Showtime's "Billions" explored virtual currencies in their most recent season, with its central character using an unnamed cryptocurrency to hide his ill-gotten trading profits, bribes and other criminal payoffs. The show featured a hardware wallet, Ledger Nano S, which is used to physically store virtual currencies, and Nano S remains thrilled about the "endorsement."

physically store virtual currencies, and Nano S remains thrilled about the "endorsement."

Bitcoin has also enjoyed references on "The Big Bang Theory" and "The Good Wife," and honorary mentions on "The Simpsons," "Jeopardy," "Silicon Valley," "House of Cards," "Supernatural," "Family Guy" — the list goes on.

But cryptocurrency visionaries and financiers leaping aboard the cryptocurrency bandwagon are in trouble. A recent bulletin from the eminent law firm Arnold & Porter sums this notion up perfectly:

> If there was ever a regulatory grace period for virtual currencies and blockchain technology, it is officially over. Five federal regulators — The Financial Crimes Enforcement Network of the US Treasury Department (FinCEN), the Securities and Exchange Commission (SEC), the Commodity Futures Trading Commission (CFTC), the Internal Revenue Service (IRS) and the Office of Foreign Assets Control (OFAC) — all recently issued statements or took actions in which they clarified their positions on the scope of their jurisdiction over multiple aspects of virtual currency and certain types of blockchain enterprises. State, foreign and multilateral regulators have also taken actions to reign in virtual currencies. Companies and investors that are now working with these technologies, or that are exploring how they might fit into their existing business strategies, must be ready to justify their activities on a comprehensive basis from regulatory, compliance, tax and business perspectives.

Not to mention that for the most part, the entire cryptocurrency system resides amid an unregulated, mysterious and arguably sinister environment — certainly unnecessary risks for a state like Ohio, whose investment strategy should be reliable, conservative and stable.

This is probably why the club of commercial enterprises most interested in accepting cryptocurrency is of an ilk not typically including state governments. For instance, at present, there is a notable (or perhaps better described as "notorious") group of merchants and customers, who are willing to put up with cryptocurrency's many logistical and regulatory inconveniences, including:

- U.S. marijuana dispensaries and users, who are not adequately served by banks because of legal problems;
- Ransomware purveyors, who cannot resist the appeal of cryptocurrency's pseudo anonymity (though ransomware schemers have reportedly become increasingly confounded by bitcoin price fluctuations and are apparently shifting to other less traditional so-called "alt coins");
- Dark web companies selling drugs, guns and other restricted items; and
- Despite a recent crackdown, cryptocurrency still holds an appeal for Chinese investors trying to bypass their country's monetary and currency restrictions.

What also bothers me about Ohio’s entrance into the seedy and unregulated world of bitcoin is that it seems more of a political ploy and publicity grab, rather than an earnest attempt at benefiting Ohio taxpayers and businesses.

Ohio State Treasurer Josh Mandel is a decorated Iraqi war veteran who served two tours, and based on public reports, seems to be doing a terrific job in Ohio, ushering in an era of transparency and accountability that has garnered tangible results. However, Mandel has also unfortunately made the Ohio bitcoin effort more about himself than about Ohio. He seems to have acted almost unilaterally and his name appears everywhere throughout the crypto process — even in the self-serving OhioCrypto.com FAQs, which read more like a campaign stump speech than objective taxpayer guidance:

> Why did the Treasurer’s office create OhioCrypto.com?
>
> Treasurer Mandel believes in leveraging cutting-edge technology to provide Ohioans more options and ease while interfacing with state government. The Treasurer’s office is also working to help make Ohio a national leader in blockchain technology.

> Treasurer Mandel has a proven record of leveraging technology to change how citizens interact with government. In 2014, Treasurer Mandel launched OhioCheckbook.com which set a new national standard for government transparency and, for the first time in Ohio history, put all state spending information on the internet. OhioCheckbook.com has earned Ohio the #1 ranking in the country for government transparency as evaluated by the U.S. Public Interest Research Group.

Being the first U.S. state to accept bitcoin for tax payments may have gotten Mandel the national headlines every politician craves, but at what cost to the safety and security of Ohio's finances?

Mandel seems like an earnest public servant who served his country bravely and honorably. But my take is that Mandel is not a pioneer or some kind of crypto superhero. Instead, Mandel will at best go down in history as a good-hearted hypebeast who let down his guard and allowed the allure of blockchain cloud his better judgment. In the end, only time will tell.

For now, before betting the farm on digital fiscal and financial scatterlings like bitcoin (yes, scatterlings), Ohio's governor, state Legislature or even federal authorities need to find a way to push back on their crypto-loving state treasurer. It's the right thing to do — before it's too late.

John Reed Stark is the president of John Reed Stark Consulting LLC, a data breach response and digital compliance firm. Formerly, Stark served for almost 20 years in the Enforcement Division of the U.S. Securities and Exchange Commission, including 11 years as the chief of its Office of Internet Enforcement. He is the author of "The Cybersecurity Due Diligence Handbook."