Published By: Kevin M. LaCroix

THE D&O DIARY

A PERIODIC JOURNAL CONTAINING ITEMS OF INTEREST FROM THE WORLD OF DIRECTORS & OFFICERS LIABILITY, WITH OCCASIONAL COMMENTARY

Guest Post: A Roadmap for President Trump's Crypto-Crackdown

By Kevin LaCroix on July 23, 2019
Posted in Cryptocurrencies

John Reed Stark

In the following guest post, John Reed Stark takes a closer look at President Donald Trump's recent Twitter tirade against cryptocurrency and lays out a roadmap for the President to follow if his administration were to crack down on cryptocurrency. John is President of John Reed Stark Consulting and former Chief of the SEC's Office of Internet Enforcement. A version of this article previously appeared on Securities Docket. I would like to thank John for allowing me to publish his article as a guest post on this site. I welcome guest post submissions from responsible authors on topics of interest to this blog's readers. Please contact me directly if you would like to submit a guest post. Here is John's article.

****

At 8:15 PM EST on July 11th, 2019, in a thunderous tweet-storm, President Donald Trump officially lambasted bitcoin and all other cryptocurrencies:

Not surprisingly, the cryptocurrency market, which tends to feed on attention, celebrated President Trump's tweets. In fact, many in the cryptocurrency community brazenly spun President Trump's tweets as validation that cryptocurrencies have finally arrived as a staple of global finance. Coinbase CEO Brian Armstrong tweeted to his 300K+ followers:

Meanwhile, the bitcoin marketplace bought into Armstrong's glee and bitcoin's price, which had surged during the month prior, shot up more than two percent to $11,636 after the President's tweets.

Few media outlets reported the President's first-ever crypto-tirade, yet the statements were actually quite newsworthy. First off, President Trump's position aligns him most closely with an array of loud and active cryptocurrency critics and skeptics, who also happen to be some of the most virulent anti-Trump Democrats, including U.S. Congresswoman Maxine Waters (D.Ca); U.S. Senator Elizabeth Warren (D Mass.); and U.S. Congressman Brad Sherman (D.Ca.).

President Trump even went so far as to co-opt some of Congressman Sherman's arguments. Congressman Sherman (who specifically introduced articles of impeachment against President Trump) recently stated:

> *"An awful lot of our international power comes from the fact that the U.S. dollar is the standard unit of international finance and transactions," Sherman said at a meeting of the House Financial Services Committee last week . . . Clearing through the New York Fed is critical for major oil and other transactions. It is the*

announced purpose of the supporters of cryptocurrency to take that power away from us, to put us in a position where the most significant sanctions we have against Iran, for example, would become irrelevant."

President Trump is also lining up against some of his own political appointees and advisors. Last year, Steve Bannon, then White House chief strategist, boasted that digital currencies "are the future." The President's acting White House Chief of Staff, Mick Mulvaney, has also been vocal about his support of cryptocurrency and the benefits of blockchain, stating back in 2014:

"My interest in [bitcoin] is to just try and make sure that government doesn't act too soon in such a fashion that curbs the potential for bitcoin. Because I see potential for bitcoin as a medium of trade and as a transactional tool, and I'd hate to see the government make decisions early that sort of retard its growth."

Similarly, Trump-appointed SEC Commissioner Hester Pierce would also likely disagree with the President. Dubbed by crypto-fanatics as the "Crypto-Mom," a nickname given after her now infamous dissent in a decision in an SEC decision to reject an exchange-traded fund (ETF) offering exposure to bitcoin, Commissioner Pierce has become somewhat of a cryptocurrency advocate. Commissioner Peirce's dissent not only contested the disapproval of what

would have been the first exchange-traded vehicle of cryptocurrency, but it also became rallying cry for bitcoin believers who argue that it's not the role of regulators to tell investors where they can invest.

Even more significant than the political oddities of President Trump's crypto-position, are the practical ramifications for the cryptocurrency marketplace. What should the cryptocurrency industry and marketplace expect now that the White House has officially taken such a loud, clear and unqualified anti-cryptocurrency position? Broken up into two parts, this article provides a possible roadmap of the machinations of a Trump-led crypto-crackdown:

- Part one provides some critical background, discussing some of the overall risks and realities of cryptocurrency. Cryptocurrency risks are vast in scope, and do not just relate to investors who gamble their life savings on its rising price, but even more importantly, the risks also relate to U.S. citizens impacted by the legion of international thieves, murderers and other outlaws who use cryptocurrency as a tool for a chilling gamut of criminal activities; and

- Part two gets into the nitty-gritty of some of President Trump's best strategical options as he kicks off his war against bitcoin and the like, providing insight into what the cryptocurrency marketplace might face from the federal government in the coming years of the Trump administration. Part two drills down especially into how President Trump could orchestrate a federal cryptocurrency sweep, using *gatekeeper theory* to focus prosecutorial and regulatory efforts on the many cryptocurrency financial platforms, custodians and other intermediaries who control "access" to cryptocurrency markets. In other words, by taking on the conduits and go-betweens that cryptocurrency users pay to trade and convert the cryptocurrency obtained from their extortion schemes, murder plots and other nefarious activities, President Trump could have a dramatic impact upon the cryptocurrency marketplace.

Part One: The Dark Side of Cryptocurrency

Need a fake I.D., a bottle of opiates, a cache of credit card numbers or a thousand social security numbers? Need a way to collect a ransomware payment? Need to fund terrorist-related activities? Need to hire a hitman? Need to finance an election tampering scheme? Cryptocurrencies like bitcoin have become the payment method of choice for these, and a slew of other, criminal enterprises.

What exactly is bitcoin? Bitcoin is a *virtual* or *digital currency* that uses encryption techniques for governance and security and operates independent of any central bank. A token is a digital asset that can be used in many ways — for example, as a unit of value (or as means of providing access to and transactional value inside a particular blockchain system (e.g., retail allows access to electronic data storage space in Sia's blockchain ecosystem). Tokens are built on top of blockchain technology, a form of distributive ledger technology, which is a digital database that is consensually shared and synchronized across networks spread across multiple sites, institutions or geographies. The U.S. government has never recognized bitcoin as a currency – rather, bitcoin and all other cryptocurrencies are simply property or, as lawyers would say, *chattel*.

Transactions in cryptocurrencies like bitcoin are pseudo-anonymous, encrypted and decentralized by nature, offering a convenient method of transferring funds obtained from illegal activities without an audit trail. Cryptocurrencies also operate outside of traditional and established financial networks and are alarmingly unregulated. There is no central issuer of bitcoins, nor a *Federal Reserve of Bitcoins* monitoring and tracking transactions or controlling their value. In short, government surveillance and regulation of cryptocurrency is virtually nonexistent (no pun intended).

Cryptocurrency transactions can create challenging hurdles for law enforcement to identify criminals. Theoretically, anyone with an Internet connection and a digital wallet can be part of any cryptocurrency platform, initial coin offering (ICO) or other cryptocurrency financing endeavor operating anywhere on the globe – which, of course, opens the laundry room door for those with criminal motives. Not surprisingly, recent data from Kapersky CiperTrace shows criminals have laundered $2.5 billion worth of criminally utilized bitcoin through cryptocurrency "exchanges," and 97% of it ends up in countries notorious for lax money laundering enforcement.

For example, when special counsel Robert Mueller indicted twelve Russian intelligence officials for allegedly attempting to influence U.S. elections in 2016 back in July, 2018, unnoticed by most in the indictment was the role of bitcoin in the crimes. The indictment notes that the conspirators used bitcoin to fund the purchase of servers, register domains, and make other payments "in furtherance of hacking activity." According to the indictment, the "use of bitcoin allowed the Conspirators to avoid direct relationships with traditional financial institutions, allowing them to evade greater scrutiny of their identities and sources of funds."

Cryptocurrency and Terrorism Financing

Much like organized criminals, terrorist organizations can use bitcoin or other cryptocurrencies to purchase a range of weaponry, including firearms or bomb-making materials, or even false passports on the dark web. A study by RAND Europe, "Behind The Curtain: The Illicit Trade Of Firearms, Explosives and Ammunition on The Dark Web," identified 24 French and British crypto-markets on the dark web during a week-long data collection period in September 2016, of which 75 per cent were found to have evidence of arms dealing.

Along these lines, the Palestinian military-political group Hamas, which the U.S. government deems a terrorist organization, may be using the Coinbase cryptocurrency exchange for fundraising. In December 2017, a woman was arrested in New York for allegedly obtaining $62,000 in bitcoin to send to Islamic State. Around the same time, an Islamic State-affiliated Darknet site called *Isdarat* sought bitcoin contributions from supporters. Recently, on June 27, 2019, Rabat, the Moroccan Central Bureau of Judicial Investigation, arrested a Palestinian national residing in the city of Mohammedia suspected of trading bitcoin for terrorist organizations.

Spotlight: Cryptocurrency and Ransomware Extortion Schemes

One of the more prominent criminal uses of bitcoin involves so-called "ransomware" schemes and provides the most glaring example of how nefarious cryptocurrency has become.

Insurer Beazley Group in its May 2019 *Beazley Breach Insights Report* (BBR) writes that its clients have reported twice the number of ransomware cyberattacks in the first quarter of 2019 as they did last year, with hackers targeting bigger companies and demanding bigger ransoms than ever before. According to the May 2019 BBR, in Q1 2019, the average reported ransomware demand was $224,871, an increase of 93% over the 2018 average of $116,324. The FBI's 2018 Internet Crime Report, is even more foreboding, stating that there were 1,493 ransomware cases reported in 2018 costing each victim on average $3.6 million. Here is how a typical ransomware extortion scheme works:

- Ransomware attackers break into a corporate system and encrypt, or lock-up, a corporate victim's data. Most ransomware infections come from phishing attacks, in which unwitting users are enticed to open a file or click on a link containing the ransomware malware;

- The ransomware attackers demand payment in cryptocurrency for the encryption key to enable the victim corporation to unlock the now inaccessible data;

- The ransomware victim pays the cryptocurrency ransom to the attacker; and

- The ransomware attackers move on to their next victim.

While ransomware attacks come in many forms, in each case they infect a computer and restrict users' access to certain data, systems, and files, until a ransom is paid. What makes ransomware attacks so devastating is that many variants do not simply target individual endpoints, but rather establish a foothold on one device and then fan out across a corporate network, encrypting everything from shared drives and email servers to website platforms and backup servers. In this way, ransomware attackers can cripple significant portions, or even all, of a company's technologically facilitated operations. Hence ransomware's dirty little secret: most corporations pay the ransom.

How do most corporate victims of ransomware attacks pay the ransoms demanded? Bitcoin – it's fast, reliable, verifiable, subject to little regulation, and virtually untraceable. Ransomware purveyors even offer customer support to show victims how to tender bitcoin payments.

Bitcoin is ideal for ransomware extortion schemes. The hacker can simply watch the public blockchain to know if and when a victim has paid up. Hackers can even create a unique payment address for each victim and automate the process of unlocking their files upon a confirmed bitcoin transaction to that unique address.

Unlike the sequence of events during a kidnapping scenario, where the exchange of money arguably places criminals in their most vulnerable position, ransomware attackers facilitate pseudo-anonymity by orchestrating a bitcoin transaction process. Rarely is there ever even an arrest, let alone a successful prosecution, of a ransomware attacker. Law enforcement remains virtually powerless, and has even fallen victim themselves to ransomware extortion schemes.

Once the ransomware attackers take possession of the bitcoin payment, it can now be laundered via the Dark Web – or even to buy a pint of *avocado ice cream* at Whole Foods; a *Nantucket Rug* at Crate and Barrel or a *Zegna Quindici Tie* at Nordstrom's (all three of which reportedly have begun accepting bitcoin and other cryptocurrencies as payment for goods).

Ransomware Attacks Against U.S. Municipalities

Ransomware attacks have also now begun to plague townships, counties, cities and other municipalities across the U.S. In June and July of 2019 alone, at least three Florida cities became victims of ransomware attacks, after similar attacks on larger cities such as Atlanta, Dallas and Baltimore.

In Lake City, Florida, more than 100 years' worth of municipal records, from ordinances to meeting minutes to resolutions and City Council agendas, were locked in cyberspace for nearly a month, hijacked by unidentified hackers who encrypted the city's computer systems and demanded 42 bitcoins (more than $460,000 at the time) to pay the ransom.

Weeks after the city's insurer paid the ransom, the city has still not recovered all of its files. Lake City was the second city to agree to a large ransom within a two week period. Riviera Beach, in Florida's Palm Beach County, signed off on an extraordinary $600,000 payment around the same time, also in bitcoin.

The Village of Key Biscayne, Florida, has not publicly disclosed whether it plans to pay the perpetrators of a recent ransomware attack, while earlier this year Jackson County, Georgia paid $400,000. Atlanta's mayor testified recently to Congress that an attack last year, when the city refused to pay $51,000 in extortion demands, has cost Atlanta $7.2 million to date.

Ransomware Attacks Against Healthcare Organizations

Healthcare organizations, from hospitals and medical centers to physician practice groups and clinics, continue to constitute a large percentage of ransomware attacks.

According to a 2018 Kaspersky Lab report, "*Cyber Pulse: The State of Cybersecurity in Healthcare*," there exists a growing and continuous pattern of ransomware cybersecurity attacks plaguing organizations in the healthcare industry. The report found more than one-in-four (27%) healthcare IT employees in North America admitting that their employer has experienced a ransomware cybersecurity attack within the past year.

Just recently, within a seven day period in June 2019, five U.S. healthcare organizations reported ransomware attacks, with some providers still operating without the use of computer systems and others frantically paying the ransom to regain access to their files and systems.

Wildly Absurd and Oft Manipulated Crypto-Valuations

The criminalities associated with cryptocurrency's use are almost as egregious and disturbing as the criminalities associated with its valuations. Bitcoin and other cryptocurrency's anarchistic valuations remain generally unregulated and without any meaningful oversight, leaving them easily susceptible to fraud and chicanery by insiders, management and better-informed traders and market participants.

For example, researchers from the University of Texas found that manipulation in the cryptocurrency market is rampant and much of the run-up in Bitcoin's price during 2017 was due to manipulation orchestrated by the Hong Kong exchange Bitfinex. In a 66-page paper, the authors found that tether was used to buy bitcoin at key moments when it was declining, which helped "stabilize and manipulate" the cryptocurrency's price. This is yet another reason for bitcoins wildly fluctuating valuations – which during in the past two years has gone from $19,000 to $3,200 and back up to over $11,000.

Liquidity Risks

The logistics of accepting cryptocurrency are unique, complicated and problematic. It is not as if a company can stroll across the street and convert cryptocurrency to U.S. dollars, record the data in a firm's accounting software, and be back in time for lunch. First, the company must identify a reliable and trustworthy financial institution to safeguard the cryptocurrency (and to convert the cryptocurrency upon demand). Where to find this kind of honorable, respected and U.S. financial institution? Not among Wall Street's traditional ranks of federally registered, regulated and monitored reliable institutions. The institutions servicing cryptocurrency clients are barely in their infancy, and unlike traditional Wall Street financial institutions, are generally not federally licensed in any way, shape or form.

Likewise, the SEC does not review the trading protocols used by these platforms, which determine how orders interact and execute, and access to a platform's trading services may not be the same for all users. For the typical cryptocurrency trading platform, there is no central regulatory authority; no state or federal team of bank auditors and compliance experts scrutinizing transactions and policing for manipulation; and no existing federal licensure – it's not just the Wild West, it's global economic anarchy.

Cybersecurity Risks

Transacting in bitcoin carries with it extraordinary cybersecurity risk. Bitcoin's true believers tout that cryptocurrencies provide a safe and secure way of making payments, but rarely have a clue as to how they work.

In 2016, hackers stole $72 million worth of bitcoin from exchange Bitfinex. And in 2018, hackers stole $500 million in digital tokens from exchange Coincheck. Binance, one of the largest cryptocurrency trading platforms in the world, just announced that hackers stole $40 million worth of bitcoin from them using a phishing and virus scheme, in what the company described as a "large scale security breach." According to the Wall Street Journal, more than $1.7 billion in cryptocurrency has been stolen over the years, most of which has come from exchanges and been centered around Asia.

Hackers have now become virtual bank robbers – except their break-ins can be done thousands of miles away from a dark and hidden basement. Renowned security technologist Bruce Scheier explains in clear and simple terms the cybersecurity risks of cryptocurrency, emphasizing bitcoin's (and blockchain's) regulatory and enforcement vacuum:

"If your bitcoin exchange gets hacked, you lose all of your money. If your bitcoin wallet gets hacked, you lose all of your money. If you forget your login credentials, you lose all of your money. If there's a bug in the code of your smart contract, you lose all of your money. If someone successfully hacks the blockchain security, you lose all of your money. In many ways, trusting technology is harder than trusting people."

To compound the problem, insuring against the risks of cyber-attacks has become increasingly challenging for the emerging industries of cryptocurrency trading platforms and custodians. High costs, liability limitations and the unknowns associated with immeasurable and unpredictable risks are among just a few of the hurdles for insurance companies seeking to underwrite ransomware policies.

Part Two: President Trump's Cryptocurrency Options

Legal commentators often lament that the U.S. financial regulatory structure was not designed to tackle the technical complexities of cryptocurrency, harping on the disfunction and chaos created when no single federal agency wields comprehensive authority over its many varying elements. However, what these legal commentators are missing is that cryptocurrency's jurisdictional maze and lack of precedent is actually a strength, not a weakness.

Aside from the obvious litany of federal agencies who prosecute fraud, and enjoy traditional jurisdiction over the cryptocurrency marketplace, some prosecutorial and regulatory agencies can take action even when there is an absence of fraud, charging cryptocurrency market intermediaries for operating without lawful compliance, protections and licensure in place. These include:

- Criminal prosecutorial agencies like the U.S. Department of Justice (DOJ);

- Civil enforcement agencies like the U.S. Securities and Exchange Commission (SEC) and U.S. Commodity Futures Trading Commission (CFTC); and

- Financial regulatory agencies like the U.S. Treasury Department and its incumbent Financial Crime Enforcement Network (FinCEN), Office of Foreign Assets Control (OFAC), and Internal Revenue Service (IRS).

Each of the above storied, capable and proven agencies can expend their vast jurisdictional reach to investigate and prosecute crypto-related crimes, by enforcing a mix of the licensure-related statutory weaponry of existing laws, rules and regulations already on the books.

In other words, even though he can't prove that an unsafe and dangerous car has been involved in a hit-and-run, President Trump still has the tools to take that car off the road.

Gatekeeper Theory

For starters, President Trump should steal a page from the playbook of perhaps the most famous and successful SEC enforcement director in history: The Honorable Stanley Sporkin. Director of the SEC Enforcement Division from 1974 to 1981; general counsel to the Central Intelligence Agency from 1981 to 1986; and U.S. District Court Judge for the District of Columbia from 1985 to 2000.

Stanley Sporkin, director of Division of Enforcement of the Securities Exchange Commission is shown in his office in Washington, Dec. 12, 1977.

Judge Sporkin championed the principle of what has come to be known as "gatekeeper liability," premised upon what he referred to as the "access theory" of regulation and enforcement. Judge Sporkin's decree: Instead of pursuing every bad actor, opt instead to achieve better, faster and more effective results in the long run by pursuing those who control "access" to our capital markets. Judge Sporkin's concept of gatekeeper enforcement leverages varying resources while also packing the most powerful punch.

In the cryptocurrency marketplace, the most obvious targets for a gatekeeper assault include:

- Cryptocurrency platforms (including so-called cryptocurrency exchanges) who allow for the conversion of bitcoin and other cryptocurrencies into dollars;

- Crypto-custodial services who provide digital wallet and other storage solutions for customers to safeguard and warehouse their cryptocurrency; and

- Corporate crypto-facilitators, who manage crypto-transactions for retailors and other companies seeking to accept cryptocurrency as payment for goods or services.

The best reason for gatekeeper theory? In stark contrast to the hackers and other cyber-criminals who go to extreme efforts to conceal their identities, crypto-gatekeepers actually *want to be found*.

Crypto-intermediaries market their services aggressively, especially online and via social media. Moreover, the Internet renders crypto-intermediary culprits easier to surveil, easier to track, and ultimately, easier to catch. This may yet prove to be the most profound change brought by the Internet on the field of law enforcement and financial regulation. Far from tying the hands of investigators and prosecutors, the Internet has evolved into the virtual rope that crypto-gatekeepers may use to hang themselves.

The most effective statutory tools for enforcement against crypto-gatekeepers are the statutes, rules and regulations relating to: 1) anti-money laundering (AML) and know your customer (KYC); 2) marketing, sale and trading of securities; and 3) federal taxation.

AML and KYC

Pursuant to the Bank Secrecy Act (BSA), transactions involving traditional financial firms, such as banks, brokers and dealers, and money service businesses (MSBs), are subject to strict federal and state 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.

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, 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 are broadly defined, and 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. 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.

The BSA 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. Since cryptocurrency financial intermediaries provide financial services, they are also mandated by AML regulations to verify their customer's identity before offering their services, also known as KYC.

Many financial institutions often blur the lines between KYC processes and AML practice. In KYC, each client is required to provide verifiable and credible identification credentials in order to use a cryptocurrency company's service. *Customer Due Diligence*(CDD) is a basic KYC process where customer's data such as proof of identity and address is gathered and used to evaluate the customer's risk profile. *Enhanced Due Diligence*(EDD) is an advanced KYC procedure for high-risk customers, prone to money laundering and financing of terrorism. Transaction monitoring is a key element of EDD.

AML programs typically include a system of internal controls to ensure ongoing compliance with the BSA; independent testing of BSA/AML compliance; a designated BSA compliance officer to oversee compliance efforts; training for appropriate personnel; and a customer identification program. Thus, to ensure AML compliance, financial firms start with KYC, by obtaining clearly identifiable information about a prospective client, and identifying any potential risks of association.

For cryptocurrency intermediaries, this would require, among other things, meticulously recording transactions; definitively knowing who customers are; and promptly and efficiently reporting suspicious activity to law enforcement.

Cryptocurrency Firms, AML and KYC

FinCEN's AML requirements combined with state law MSB licensing and bonding requirements create a hefty, burdensome and onerous federal and state regulatory burden and concern for crypto-intermediaries**.**

For instance, when a cryptocurrency intermediary conducts business with suspicious individuals, their actions could raise AML red flags and violate *FinCEN's Guidance on the Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies*.

President Trump could announce a "federal cryptocurrency sweep" and direct that cryptocurrency firms be subject to on-site audits 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.

Given the identification and verification challenges associated with the global locations, pseudo-anonymity, encryption, decentralization and historically criminal tendencies of typical cryptocurrency users, a federal sweep of cryptocurrency intermediaries will likely identify a plethora of AML, KYC and other BSA violations. Not only do cryptocurrency firms

typically lack the sophisticated technological compliance infrastructure of traditional U.S. financial institutions, but they are also misguided when it comes to their AML/KYC and other related BSA compliance responsibilities.

Letitia James
NY Attorney General

OUR OFFICE MEDIA RESOURCES INITIATIVES

Home » Media Center » Press Releases » April 17th 2018

Español

A.G. Schneiderman Launches Inquiry Into Cryptocurrency "Exchanges"

Virtual Markets Integrity Initiative Seeks to Improve Transparency and Accountability of Major Cryptocurrency Trading Platforms to Protect Virtual Currency Investors

AG's Office Sends Letters to 13 Virtual Currency Trading Platforms or "Exchanges" Requesting Disclosures on Their Operations, Use of Bots, Conflicts of Interest, Outages, and Other Key Issues

Today, New York Attorney General Eric T. Schneiderman launched the Virtual Markets Integrity Initiative, a fact-finding inquiry into the policies and practices of platforms used by consumers to trade virtual or "crypto" currencies like bitcoin and ether. As part of a broader effort to protect cryptocurrency investors and consumers, the Attorney General's office sent letters to thirteen major virtual currency trading platforms requesting key information on their operations, internal controls, and safeguards to protect customer assets. As the letters explain, the Initiative seeks to increase transparency and accountability as it relates to the platforms retail investors rely on to trade virtual currency, and better inform enforcement agencies, investors, and consumers.

Along these lines, the New York State Attorney General's office (NYAG) asked 14 popular crypto trading platforms to respond to answer 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 connection between cryptocurrency and money laundering — as well as a range of market manipulation concerns.

U.S. law enforcement agencies have already vowed to crack down on the cryptocurrency custodian and conversion firms who serve criminals, even those operating outside the United States. DOJ, 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.

Indeed, 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, a bitcoin exchange operator, 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 benefitted 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."*

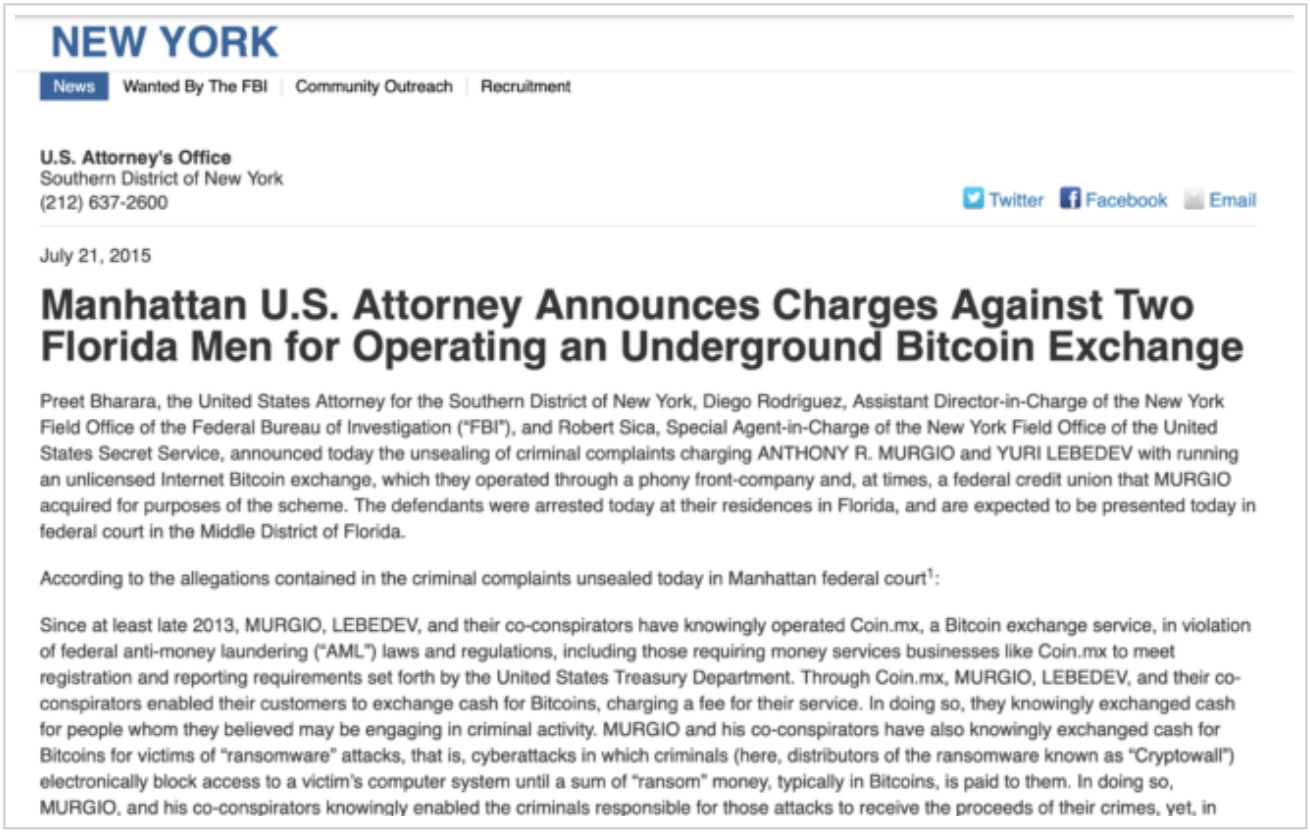
Anthony Murgio of Tampa, 33, was sentenced Tuesday to 5 1/2 years in prison for running a Bitcoin exchange suspected of laundering money for a group of hackers who targeted publishing and financial firms as part of a complex securities fraud. [AP photo]

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 the Financial Crimes Enforcement Network (FinCEN);
- Maintain an effective AML program;

- Comply with AML record-keeping requirements; and

- File with FinCEN *Suspicious Activity Reports* (SARs) regarding customers who use cryptocurrencies for nefarious purposes.



NEW YORK

News | Wanted By The FBI | Community Outreach | Recruitment

U.S. Attorney's Office
Southern District of New York
(212) 637-2600

Twitter Facebook Email

July 21, 2015

Manhattan U.S. Attorney Announces Charges Against Two Florida Men for Operating an Underground Bitcoin Exchange

Preet Bharara, the United States Attorney for the Southern District of New York, Diego Rodriguez, Assistant Director-in-Charge of the New York Field Office of the Federal Bureau of Investigation ("FBI"), and Robert Sica, Special Agent-in-Charge of the New York Field Office of the United States Secret Service, announced today the unsealing of criminal complaints charging ANTHONY R. MURGIO and YURI LEBEDEV with running an unlicensed Internet Bitcoin exchange, which they operated through a phony front-company and, at times, a federal credit union that MURGIO acquired for purposes of the scheme. The defendants were arrested today at their residences in Florida, and are expected to be presented today in federal court in the Middle District of Florida.

According to the allegations contained in the criminal complaints unsealed today in Manhattan federal court[1]:

Since at least late 2013, MURGIO, LEBEDEV, and their co-conspirators have knowingly operated Coin.mx, a Bitcoin exchange service, in violation of federal anti-money laundering ("AML") laws and regulations, including those requiring money services businesses like Coin.mx to meet registration and reporting requirements set forth by the United States Treasury Department. Through Coin.mx, MURGIO, LEBEDEV, and their co-conspirators enabled their customers to exchange cash for Bitcoins, charging a fee for their service. In doing so, they knowingly exchanged cash for people whom they believed may be engaging in criminal activity. MURGIO and his co-conspirators have also knowingly exchanged cash for Bitcoins for victims of "ransomware" attacks, that is, cyberattacks in which criminals (here, distributors of the ransomware known as "Cryptowall") electronically block access to a victim's computer system until a sum of "ransom" money, typically in Bitcoins, is paid to them. In doing so, MURGIO, and his co-conspirators knowingly enabled the criminals responsible for those attacks to receive the proceeds of their crimes, yet, in

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.

Following up on the Murgio prosecution, DOJ announced in April 30, 2019, that it charged two individuals with bank fraud in connection to a system for depositing funds to cryptocurrency trading platforms. In a statement, the U.S. Attorney's Office for the Southern District of New York alleged that Reginald Fowler of Arizona and Ravid Yosef, said

to live in Tel Aviv, Israel, were part of a scheme that involved using bank accounts to move money into a series of unnamed cryptocurrency trading platforms.

The Financial Crimes Enforcement Network (FinCEN), working in coordination with the U.S. Attorney's Office for the Northern District of California, assessed a $110 million fine against BTC-e a/k/a Canton Business Corporation (BTC-e) for willfully violating U.S. anti-money laundering (AML) laws. Russian national Alexander Vinnik, one of the operators of BTC-e, was arrested in Greece this week, and FinCEN assessed a $12 million penalty against him for his role in the violations.

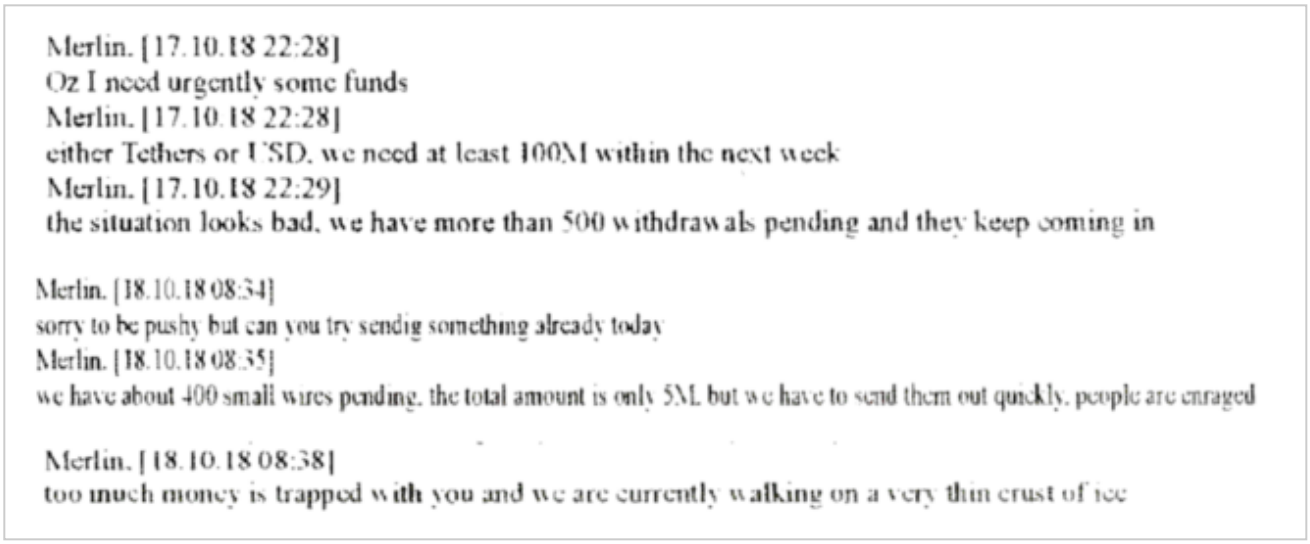
BTC-e is an internet-based, foreign-located money transmitter that exchanges fiat currency as well as the convertible virtual currencies Bitcoin, Litecoin, Namecoin, Novacoin, Peercoin, Ethereum, and Dash. It is one of the largest virtual currency exchanges by volume in the world. BTC-e facilitated transactions involving ransomware, computer hacking, identity theft, tax refund fraud schemes, public corruption, and drug trafficking.

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."*

Some states have already taken the lead in prosecuting AML-related violations at cryptocurrency firm. For example, on April 26, 2019, the New York Attorney General accused the owners of a prominent cryptocurrency trading platform, Bitfinex, of using illicit transactions to mask $850 million in missing funds. According to a 23-page legal filing, Bitfinex raided the reserves of a so-called stablecoin called Tether — a digital currency purportedly backed one-to-one by U.S. dollars—in order to pay out customers demanding withdrawals from the platform.

The New York AG filing also reproduces messages written by a Bitfinex executive which plead for capital from a Panamanian payment processor to which it had transferred funds. The exact identity of the Panamanian payment processor, Crypto Capital, is unclear. According to the attorney general, Bitfinex, which is incorporated in the British Virgin Islands, relied on a shadowy network of money agents, including "human being friends of Bitfinex employees that were willing to use their bank accounts to transfer money to Bitfinex clients."


Merlin. [17.10.18 22:28]
Oz I need urgently some funds
Merlin. [17.10.18 22:28]
either Tethers or USD. we need at least 100M within the next week
Merlin. [17.10.18 22:29]
the situation looks bad. we have more than 500 withdrawals pending and they keep coming in

Merlin. [18.10.18 08:34]
sorry to be pushy but can you try sendig something already today
Merlin. [18.10.18 08:35]
we have about 400 small wires pending. the total amount is only 5M but we have to send them out quickly. people are enraged

Merlin. [18.10.18 08:38]
too much money is trapped with you and we are currently walking on a very thin crust of ice

Clearly, the noxious mix of AML and MSB federal and state regulatory requirements not only creates a foggy, deadly compliance labyrinth for any cryptocurrency firm – but is also replete with risk for anyone (or any U.S. state) doing business with them. This creates the perfect opportunity for President Trump to add federal investigatory and enforcement muscle into the mix.

Money Transmitter Registration

President Trump also enjoys a lesser known (and oft misunderstood) jurisdictional "hook" when cryptocurrency intermediaries run afoul with state registration of so-called money transmitters.

A subset of the larger group of MSBs, a money transmitter is typically defined to include a person that "provides money transmission services, or any other person engaged in the transfer of funds." The term "money transmission services" means "the acceptance of currency, funds, or other value that substitutes for currency from one person *and* the transmission of currency, funds, or other value that substitutes for currency to another location or person by any means."

Failure to register as a money transmitter in a state can, under certain conditions, trigger DOJ criminal prosecutorial jurisdiction. Pursuant to 18 US Code §1960, captioned *Prohibition of Unlicensed Money Transmitting Businesses*:

"Whoever knowingly conducts, controls, manages, supervises, directs, or owns all or part of an unlicensed money transmitting business, shall be fined in accordance with this title or imprisoned not more than 5 years, or both."

Section 1960 lists three categories of unlicensed money transmitting businesses, which are, in summary:

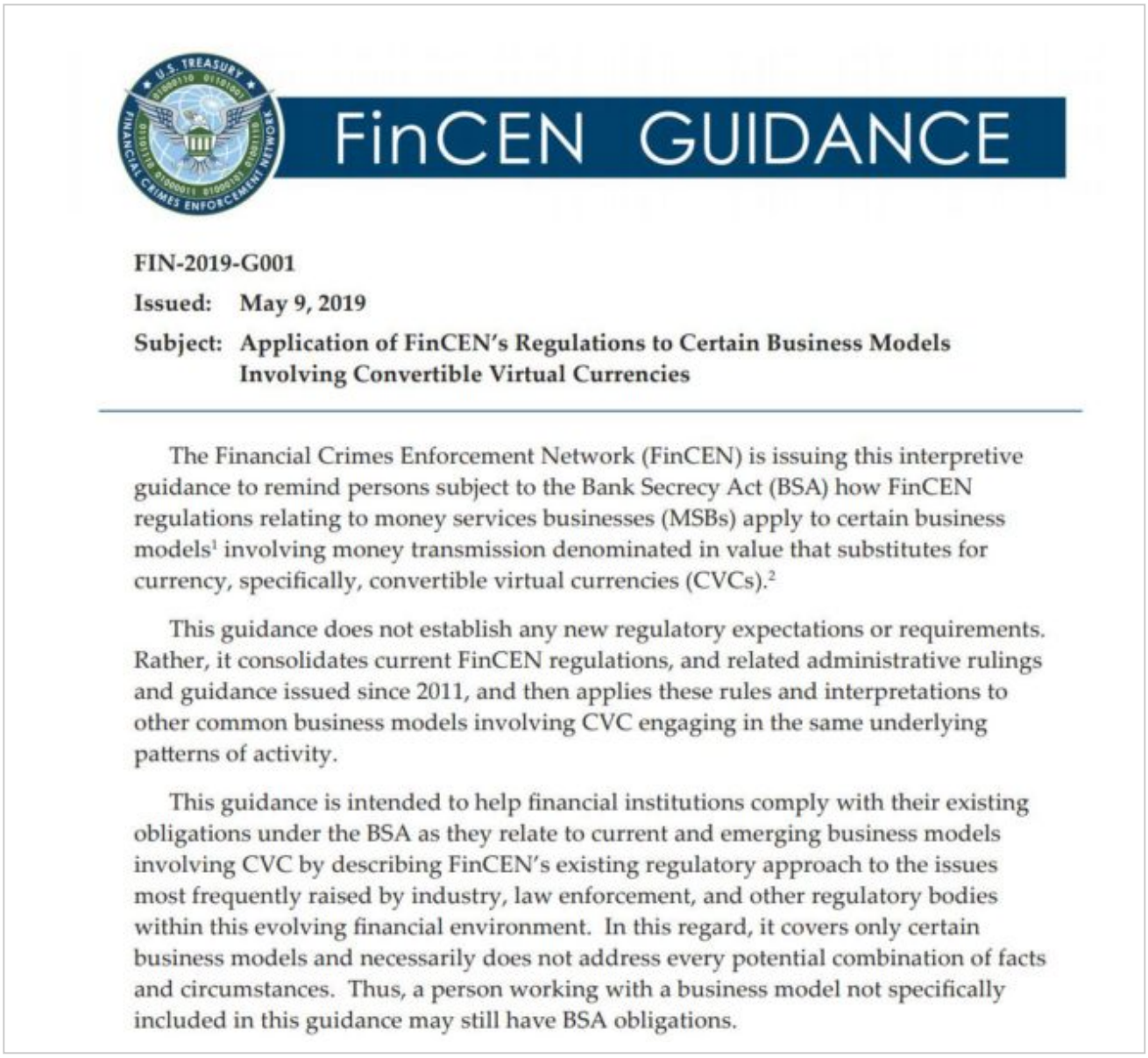
- Those operating in a state that requires that business to be licensed and makes it a misdemeanor or felony not to do so;

- Those that fail to comply with Treasury Department regulations covering such a business (e.g., registering with FinCEN); and

- Those that transmit money known to the transmitter to come from or intended to finance criminal activity.

In most instances, Section 1960 does not require specific intent. As part of the USA Patriot Act, Congress amended Section 1960(b)(1)(A) to provide that a defendant can be convicted of operating an unlicensed money transmitting business "whether or not the defendant knew that the operation was required to be licensed or that the operation was so punishable." This strict liability paradigm is a formidable contrivance for investigators and prosecutors, who can allege liability regardless of the intent or mental state of the perpetrator. (Many drug possession crimes and statutory rape are examples of other strict liability crimes.)

Recent FinCEN Guidance, DApps, Kiosks and Other Crypto-Payment Processors



FinCEN GUIDANCE

FIN-2019-G001

Issued: May 9, 2019

Subject: Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies

The Financial Crimes Enforcement Network (FinCEN) is issuing this interpretive guidance to remind persons subject to the Bank Secrecy Act (BSA) how FinCEN regulations relating to money services businesses (MSBs) apply to certain business models[1] involving money transmission denominated in value that substitutes for currency, specifically, convertible virtual currencies (CVCs).[2]

This guidance does not establish any new regulatory expectations or requirements. Rather, it consolidates current FinCEN regulations, and related administrative rulings and guidance issued since 2011, and then applies these rules and interpretations to other common business models involving CVC engaging in the same underlying patterns of activity.

This guidance is intended to help financial institutions comply with their existing obligations under the BSA as they relate to current and emerging business models involving CVC by describing FinCEN's existing regulatory approach to the issues most frequently raised by industry, law enforcement, and other regulatory bodies within this evolving financial environment. In this regard, it covers only certain business models and necessarily does not address every potential combination of facts and circumstances. Thus, a person working with a business model not specifically included in this guidance may still have BSA obligations.

FinCEN recently published on May 9, 2019, a new guidance sheet entitled, "Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies," outlining when and how different companies, individuals and platforms in the cryptocurrency marketplace may be money transmitters under the BSA and other relevant laws. The interpretive guidance also concurrently issued an advisory about possible illicit activity and suspicious transactions relating to the use of virtual currencies.

FinCEN's guidance provides a useful roadmap of the many different cryptocurrency payment processors whose actions likely trigger money transmitter regulations and licensure, including cryptocurrency transactions provided through:

- Cryptocurrency Kiosks and ATMS, which are scattered throughout the country and typically operate in a very suspicious and dangerous manner. According to FinCEN, owners and operators of CVC [cryptocurrency] kiosks that utilize electronic terminals to receive real currency from consumers and to transfer the equivalent value in cryptocurrency (or vice versa) are deemed to be money transmitters;
- P2P exchanges, which are decentralized exchanges operated and maintained by software that typically involve natural persons engaged in buying and selling cryptocurrencies. P2P could involve transferring one type of cryptocurrency for a different type of cryptocurrency or exchanging cryptocurrency for other types of value (like fiat). Unless a P2P exchanger is "a natural person engaging in such activity on an infrequent basis and not for profit or gain" such person who "engages in money transmission services involving real currency or CVC [cryptocurrency] must comply with BSA regulations as a money transmitter;" and
- Decentralized (distributed) applications, (DApps), which are software programs that operate on a P2P network of computers running a blockchain platform, which perform a wide variety of functions, including providing financial services. Generally, a DApp user must pay a fee to the DApp (for the ultimate benefit of the owner/operator) in order to run the software, which is commonly paid in cryptocurrency. When DApps perform money transmission, the DApp and/or its owners/operators, are considered money transmitters and subject to BSA requirements.

FinCEN also mentions that cryptocurrency payment processors may not avail themselves of FinCEN's payment processor exemption from MSB registration. One of the four conditions of this exemption — all of which must be met — is that the entity must "operate through clearance and settlement systems that admit only BSA-regulated financial institutions." According to FinCEN, cryptocurrency payment processors are generally unable to meet this condition and are thus money transmitters "regardless of whether they accept and transmit the same type of cryptocurrency, or they accept one type of value (such as currency or funds) and transmit another (such as cryptocurrency)."

UNITED STATES OF AMERICA
DEPARTMENT OF THE TREASURY
FINANCIAL CRIMES ENFORCEMENT NETWORK

IN THE MATTER OF:	)	
	)	
	)	
	)	**Number 2019-01**
Eric Powers	)	
Kern County, California	)	

ASSESSMENT OF CIVIL MONEY PENALTY

I. INTRODUCTION

The Financial Crimes Enforcement Network (FinCEN) has determined that grounds exist to assess a civil money penalty against Eric Powers, pursuant to the Bank Secrecy Act (BSA) and

FinCEN's recent cryptocurrency guidance follows its first enforcement action against a "peer-to-peer cryptocurrency exchanger" for breaking AML rules, filed April 18, 2019, only a month before FinCEN issued the new guidance.

Specifically, FinCEN assessed a civil money penalty against Eric Powers for willfully violating BSA registration, program, and reporting requirements. Powers failed to register as an MSB, had no written policies or procedures for ensuring compliance with the BSA, and failed to report suspicious transactions and currency transactions.

Powers operated as a peer-to-peer exchanger of convertible virtual currency. Powers advertised his intent to purchase and sell bitcoin online and completed transactions by either physically delivering or receiving currency in person, sending or receiving currency through the mail, or coordinating transactions by wire through a depository institution. Powers processed numerous suspicious transactions without ever filing a SAR, including doing business related to the illicit darknet marketplace "Silk Road," as well as servicing customers through The Onion Router (TOR) without taking steps to determine customer identity and whether funds were derived from illegal activity.

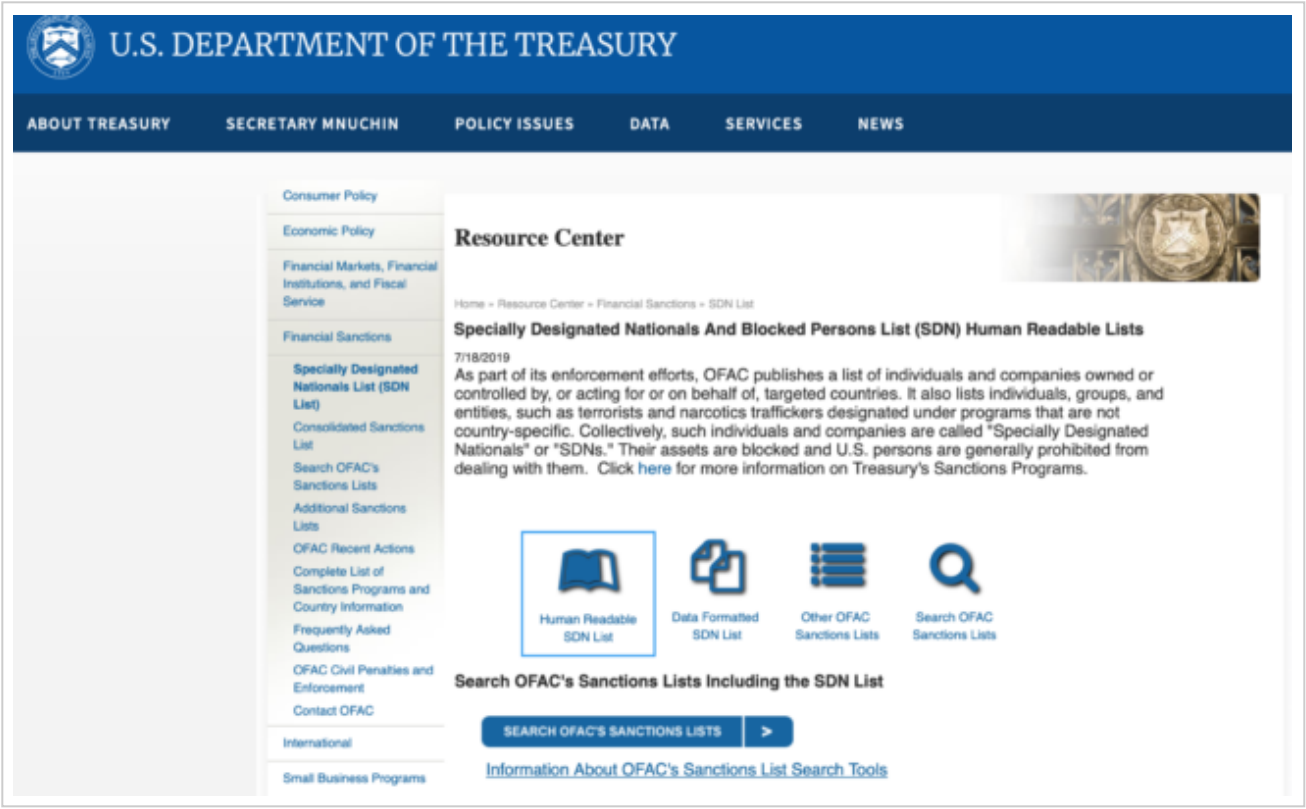
Powers conducted over 200 transactions involving the physical transfer of more than $10,000 in currency, yet failed to file a single CTR. For instance, Powers conducted approximately 160 purchases of bitcoin for approximately $5

million through in-person cash transactions, conducted in public places such as coffee shops, with an individual identified through a bitcoin forum. Of these cash transactions, 150 were in-person and were conducted in separate instances for over $10,000 during a single business day. Each of these 150 transactions necessitated the filing of a CTR.

FinCEN Director Kenneth A. Blanco stated at the time:

> *"It should not come as a surprise . . . that exchangers of convertible virtual currency, such as Mr. Powers, are money transmitters and must register as MSBs . . . Such failures put our financial system and national security at risk and jeopardize the safety and well-being of our people, as well as undercut responsible innovation in the financial services space."*

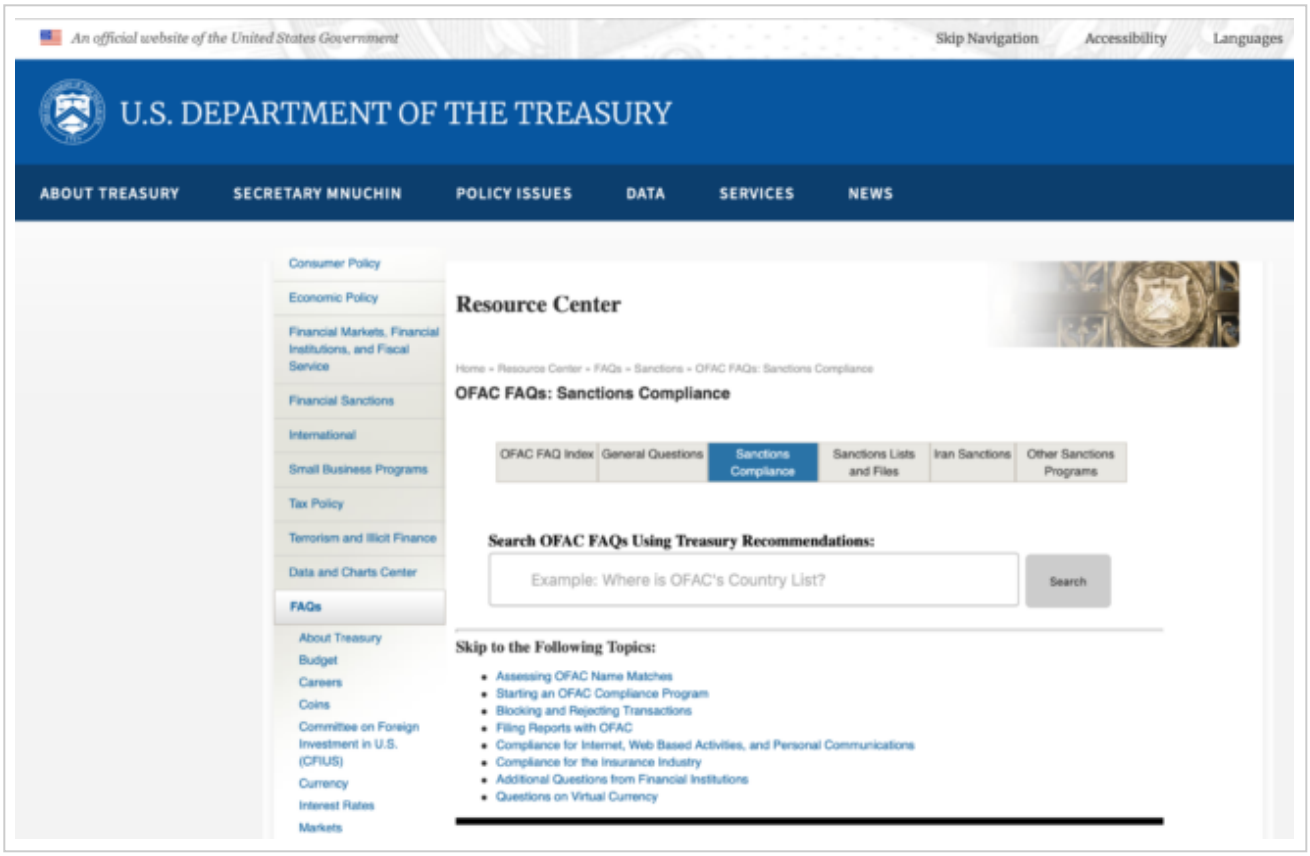
Cryptocurrency and OFAC



Aside from AML and KYC requirements, the U.S. Treasury's Office of Foreign Assets Control (OFAC) also requires cryptocurrency financial intermediaries to conduct specific verification processes for offshore taxpayers.

OFAC administers and enforces economic and trade sanctions based on US foreign policy and national security goals against targeted foreign countries and regimes, terrorists, international narcotics traffickers, those engaged in activities related to the proliferation of weapons of mass destruction, and other threats to the national security, foreign policy or economy of the United States. OFAC acts under Presidential national emergency powers, as well as authority granted by specific legislation, to impose controls on transactions and freeze assets under U.S. jurisdiction.

Many of the sanctions are based on United Nations and other international mandates, are multilateral in scope, and involve close cooperation with allied governments.



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. Every cryptocurrency firm must therefore ensure that none of its clients are on the list of prohibited individuals or entities maintained by OFAC and not based in countries subject to broader economic sanctions.

For its part relating to cryptocurrencies, OFAC recently released guidance, issued in the form of Frequently Asked Questions (FAQs). The FAQs explain that transactions involving cryptocurrencies will be treated the same as other transactions — a position that multiple Treasury Department officials have signaled before, dating back to as early as February 2018.

Notably, in late November, 2018, 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." The decision to include digital currency

wallet addresses on OFAC's Specially Designated Nationals And Blocked Persons List (SDN) 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.

On that same day, OFAC identified two digital currency addresses associated with these two financial facilitators. 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. For instance, announced as part of a joint action with the Treasury Department, DOJ alleged that, in a SamSam ransomware scheme that targeted over 200 known victims, two Iran-based individuals "helped exchange digital currency (bitcoin) ransom payments into Iranian rial on behalf of Iranian malicious cyber actors involved with the.

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.

President Trump and AML, KYC and OFAC

Identifying the source of cryptocurrency, or in the least, confirming that the cryptocurrency is not somehow tainted by unlawful conduct, can be especially challenging. 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.

President Trump's anti-crypto team should consider that for crypto-gatekeepers like cryptocurrency firms, meeting their AML, KYC and OFAC responsibilities is a Herculean task, making charging decisions easier and providing endless prosecutorial fodder. From executive orders to presidential cheerleading, President Trump could use his position to create, promote and expand current cryptocurrency-related enforcement efforts by the Treasury Department FinCEN and DOJ, and garner significant results, without having to deplete precious federal law enforcement resources.

Marketing, Sale and Trading of Securities

In addition to prosecuting cryptocurrency firms with AML, KYC and OFAC violations, President Trump should also consider encouraging the SEC's already active cryptocurrency enforcement program to redouble their efforts applying gatekeeper theory. The SEC has already been hard at work bringing a slew of enforcement actions addressing the often bold and transparent violation of critical SEC registration requirements by cryptocurrency firms.

By way of background, most cryptocurrency financial marketplaces, platforms and intermediaries mistakenly believe that the SEC's exchange-related and brokerage-related licensing requirements do not apply to them. Thus, most:

- Are not registered with any federal government agency and would argue that they have no federal liquidity, net capital or other depository or financial requirements of any kind;

- Are not examined or audited by any federal agency such as the Federal Reserve or the U.S. Securities and Exchange Commission (SEC); and

- Are not examined or audited by any quasi-government agency such as the Financial Industry Regulatory Authority (FINRA).

Cryptocurrency Trading Platforms as Unregistered Exchanges

Put simply, a securities exchange is a company that creates the opportunity for potential buyers and sellers of a security to come together for trading – and per the SEC, cryptocurrency tokens can be securities. Hence, the need to register under Section 6 of the Exchange Act, or operate pursuant to an appropriate exemption (such as an alternative trading system that complies with Regulation ATS, which requires, among other things, registration as a broker-dealer and filing of a Form ATS with the SEC).

The federal regulatory framework governing registered national securities exchanges and exempt markets is designed to protect investors and prevent against fraudulent and manipulative trading practices. Therefore, entities providing exchange-like services are subject to *routine* and *for cause* examinations, and must:

- Carefully handle access to, and control of, investor funds;
- Maintain meticulous records of certain communications;

- Insure robust cybersecurity;

- Install a vigorous culture of compliance under a formalized and detailed compliance program; and

- Provide all users with a broad range of adequate protection and fortification.

National Securities Exchanges

A "national securities exchange" is a securities exchange that has registered with the SEC under Section 6 of the Securities Exchange Act of 1934.

Following is a list of exchanges registered with the SEC under Section 6(a) of the Exchange Act as national securities exchanges:

- BOX Exchange LLC (formerly BOX Options Exchange LLC)
- Cboe BYX Exchange, Inc. (formerly Bats BYX Exchange, Inc.; BATS Y-Exchange, Inc.)
- Cboe BZX Exchange, Inc. (formerly Bats BZX Exchange, Inc.; BATS Exchange, Inc.)
- Cboe C2 Exchange, Inc.
- Cboe EDGA Exchange, Inc. (formerly Bats EDGA Exchange, Inc.; EDGA Exchange, Inc.)
- Cboe EDGX Exchange, Inc. (formerly Bats EDGX Exchange, Inc.; EDGX Exchange, Inc.)
- Cboe Exchange, Inc.
- The Investors Exchange LLC
- Miami International Securities Exchange
- MIAX Emerald, LLC
- MIAX PEARL, LLC
- Nasdaq BX, Inc. (formerly NASDAQ OMX BX, Inc.; Boston Stock Exchange)
- Nasdaq GEMX, LLC (formerly ISE Gemini)
- Nasdaq ISE, LLC (formerly International Securities Exchange, LLC)
- Nasdaq MRX, LLC (formerly ISE Mercury)
- Nasdaq PHLX LLC (formerly NASDAQ OMX PHLX, LLC; Philadelphia Stock Exchange)
- The Nasdaq Stock Market
- New York Stock Exchange LLC
- NYSE Arca, Inc.
- NYSE Chicago, Inc. (formerly Chicago Stock Exchange)
- NYSE MKT LLC (formerly NYSE AMEX and the American Stock Exchange)
- NYSE National, Inc. (formerly National Stock Exchange, Inc.)

SEC exchange registration is an extraordinarily robust regulatory requirement, which is why there are only a small handful of actual SEC-registered exchanges, and makes the group an exclusive fraternity of responsible and rock-solid financial institutions.

Cryptocurrency intermediaries often give the impression to investors that they meet the SEC regulatory standards of national securities exchanges and that their operations are similarly transparent, reliable, trustworthy and bonafide. This is not true.

Many cryptocurrency trading platforms even go so far as to refer to themselves as "exchanges," though they bear little resemblance to the traditional securities exchanges currently operating within U.S. markets, such as the New York Stock Exchange or the NASDAQ. The SEC became so concerned about this arguably unlawful nomenclature that they took the unusual step of issuing an official statement to address the misinformation, stating on March 18th, 2018:

> *"Many platforms refer to themselves as "exchanges," which can give the misimpression to investors that they are regulated or meet the regulatory standards of a national securities exchange. Although some of these platforms claim to use strict standards to pick only high-quality digital assets to trade, the SEC does not review these standards or the digital assets that the platforms select, and the so-called standards should not be equated to the listing standards of national securities exchanges. Likewise, the SEC does not review the trading protocols used by these platforms, which determine how orders interact and execute, and access to a platform's trading services may not be the same for all users. Again, investors should not assume the trading protocols meet the standards of an SEC-registered national securities exchange. Lastly, many of these platforms give the impression that they perform exchange-like functions by offering order books with updated bid and ask pricing and data about executions on the system, but there is no reason to believe that such information has the same integrity as that provided by national securities exchanges."*

EtherDelta

The SEC has already begun its efforts at policing unregistered exchanges in the cryptocurrency marketplace. Specifically, on November 8th, 2018, the SEC settled charges against Zachary Coburn, the founder of EtherDelta, a digital token trading platform, initiating its first SEC enforcement action based on findings that such a platform operated as an unregistered national securities exchange.

According to the SEC's order, EtherDelta is an online platform for secondary market trading of ERC20 tokens, a type of blockchain-based token commonly issued in ICOs. The SEC order found that Coburn caused EtherDelta to operate as an unregistered national securities exchange.

EtherDelta provided a marketplace for bringing together buyers and sellers for digital asset securities through the combined use of an order book, a website that displayed orders, and a "smart contract" run on the Ethereum blockchain. EtherDelta's smart contract was coded to validate the order messages, confirm the terms and conditions of orders, execute paired orders, and direct the distributed ledger to be updated to reflect a trade. Over an 18-month period, EtherDelta's users executed more than 3.6 million orders for ERC20 tokens, including tokens deemed securities under the federal securities laws.

The SEC charged that EtherDelta offered trading of various digital asset securities and failed to register as an exchange or operate pursuant to an exemption. SEC Enforcement co-director Stephanie Avakian noted sternly at the time, "EtherDelta had both the user interface and underlying functionality of an online national securities exchange and was required to register with the SEC or qualify for an exemption."

Without admitting or denying the findings, Coburn consented to the order and agreed to pay $300,000 in disgorgement plus $13,000 in prejudgment interest and a $75,000 penalty. The Commission's order recognized Coburn's cooperation, which the Commission considered in determining not to impose a greater penalty.

Cryptocurrency Trading Platforms and Broker-Dealer Registration Violations

In addition to enforcing federal registration provisions pertaining to exchanges, the SEC also enforces strict liability registration provisions pertaining to broker-dealer activity, an extremely broad and sweeping registration requirement with few, if any, exceptions.

Specifically, Section 15(a)(1) of the Securities Exchange Act of 1934 makes it unlawful for a person to "effect a transaction in securities" or "attempt to induce the purchase or sale of, any security" unless they are registered as a broker or dealer under the rules and regulations of FINRA, the regulatory organization designated by the SEC to license and regulate broker-dealers.

The ramifications for failure to register as a broker-dealer are severe, even criminal. In addition, Section 20(e) of the Exchange Act, under which the SEC may impose aiding-and-abetting liability on any person that knowingly or recklessly provides substantial assistance in a violation of the Exchange Act, creates additional potential liability. Finally, merely retaining and permitting an unlicensed intermediary to help facilitate or effect a securities transaction may be a violation of federal and many state laws and may subject others to possible civil and criminal penalties, including imprisonment.

In accordance with these fairly stringent requirements, cryptocurrency firms collecting listing fees, marketing fees, facilitation fees or any other iteration of transaction-based compensation from crypto-funding companies, could trigger broker-dealer registration.

Even if crypto-trading arrangements conceal the true intent of the relationship between any sort of funding company and the cryptocurrency trading platform, payment of transaction-based compensation i.e., a commission or some form of compensation that varies with the size or type of the resulting investment, is treated by the SEC as a nearly-conclusive indication that a person is engaged in the securities business and should be registered as a broker-dealer.

While the SEC has consistently viewed transaction-based compensation as the "hallmark" of broker dealer activity, there are a broad range of other kinds of transaction-related conduct that can trigger broker-dealer registration. Failure to register under such circumstances can render any related securities offering immediately and irrevocably tainted, even triggering rescission rights.

By skirting broker-dealer registration requirements, cryptocurrency trading platforms peddling any sort of securities offering are not adhering to a safe and transparent financial services regulatory framework. For instance, broker-dealers are required to "observe high standards of commercial honor and just and equitable principles of trade" in the conduct of its business, including determining if an investment is "suitable" for its customer and maintaining meticulous records of communications, representations, transactions and other important information.

Broker-dealers also are subject to SEC and FINRA examinations together with an exhaustive laundry list of regulations and rules of conduct as well as a rigorous training, testing and certification process.

Spotlight: IEO Services, Prima Facie Broker-Dealer Behavior

President Trump could begin his broker-dealer crypto-initiative by emboldening the SEC to target cryptocurrency trading platforms peddling increasingly popular initial exchange offerings (IEOs).

An IEO is a crypto-financing model offered and administrated via a cryptocurrency trading platform on behalf of a company (typically some form of start-up) that seeks to raise funds with its newly issued cryptocurrency digital tokens. Each IEO negotiates its unique terms, deals, and conditions with the various cryptocurrency trading platforms.

In an IEO, cryptocurrency platforms essentially become the counter-parties in the entire token offering process, enabling crypto projects to launch their offering directly on the platform (as opposed to initial coin offerings (ICOs), where the counter-parties are the fundraising company's development team that creates or "mints" the tokens). The tokens sold in an IEO are distributed to investors by the cryptocurrency platform itself (as opposed to ICOs, where the fundraising company's development team distributes the tokens).

IEO buyers/participants/investors (whatever the preferred terminology for IEO token purchaser) typically create an account on the cryptocurrency trading platform where the IEO is conducted. They then fund their digital wallets with tokens typically issued by the cryptocurrency platform, and use those cryptocurrency platform tokens to buy the fundraising company's tokens. After the cryptocurrency platform's customers purchase the fundraising company tokens directly from the trading platform, their "coins" are then "listed" on the cryptocurrency trading platform after the IEO ends.

Token issuers typically pay a listing fee to the cryptocurrency platform along with a percentage of the tokens sold during the IEO. In connection with the IEO, the cryptocurrency trading platform might provide marketing, due diligence and other facilitation services relating to the newly issued coin.

While no official data exists, the total funds raised by IEO projects globally, since inception, purportedly stands at over $1.6 billion dollars. About $518 million has been raised through 63 IEOs in 2019 through May, according to John Todaro, director of digital currency research at TradeBlock, a New York-based data provider.

Transaction-based-compensation arrangements in IEO offerings are multifaceted, including listing fee arrangements and other transaction-related payments at the outset and throughout the IEO process. Also, the cryptocurrency trading platform's own token is typically the instrument used to participate in the sale, providing an additional source of profiting opportunities.

In addition, the manner in which cryptocurrency trading platforms manage, package and market IEOs make the SEC's broker-dealer registration case even stronger (if that were possible). For example, in a typical IEO, cryptocurrency trading platforms boast of unique liquidity and marketing services such as: 1) easy access to a large potential purchaser base; 2) help with crypto-assets distribution; 3) an advertising boost from being promoted on the exchange's social media; and 4) an immediate listing on the crypto-assets exchange post-IEO.

Cryptocurrency trading platforms also tout their internal due diligence vetting of IEO issuers and as a critical benefit to engaging their facilities. Cryptocurrency platforms go so far as to hawk the "security and safety" of their respective IEOs, committing themselves to rejecting certain ineligible projects that may pose risks to investor's assets, thus creating "a safer crypto investment environment."

Given that ICOs are deemed to be offering securities, IEO facilitators and intermediaries such as cryptocurrency platforms and promoters are arguably trading securities for compensation, and would likely need to comply with SEC broker-dealer registration requirements.

To date, very few, if any, cryptocurrency trading platforms are actually registered as broker-dealers, including those peddling IEOs. By encouraging the SEC to enforce broker-dealer registration requirements, President Trump could have a rapid and significant impact upon the cryptocurrency marketplace.

Spotlight: Digital Wallet Services, Prima Facie Broker-Dealer Behavior

In addition to online trading platforms, the *SEC March 7, 2018 Statement on Potentially Unlawful Online Platforms for Trading Digital Assets* also raised concerns about companies that offer "digital wallet services" for holding or storing digital assets:

> *"Some online trading platforms may not meet the definition of an exchange under the federal securities laws, but directly or indirectly offer trading or other services related to digital assets that are securities. For example, some platforms offer digital wallet services (to hold or store digital assets) or transact in digital assets that are securities. These and other services offered by platforms may trigger other registration requirements under the federal securities laws, including broker-dealer, transfer agent, or clearing agency registration, among other things."*

Recently in a July 8, 2019 Joint Staff Statement on Broker-Dealer Custody of Digital Asset Securities, the SEC and FINRA clarified that entities seeking to participate in the marketplace for digital asset securities must comply with the relevant securities laws, most notably the customer protection rule. The SEC warned that non-registered firms would likely have to register as a broker-dealer before engaging in custodian services related to digital asset securities, noting that:

> *"The requirements of the Customer Protection Rule have produced a nearly fifty year track record of recovery for investors when their broker-dealers have failed . . . This record of protecting customer assets held in custody by*

broker-dealers stands in contrast to recent reports of cybertheft, and underscores the need to ensure broker-dealers robust protection of customer assets, including digital asset securities."

With the increasing popularity of investing in bitcoin and other cryptocurrencies, digital wallets have become a common custodial service offered by an array of cryptocurrency intermediaries. Though bitcoin and ether might not be classified as securities, by targeting digital wallet services for SEC registration violations, President Trump could significantly impact the cryptocurrency marketplace, potentially crippling an important access point of cryptocurrency users.

President Trump and Investor Protection

By supporting an SEC-led crypto-crackdown, President Trump would not only be preventing crypto-related crimes, he would be accomplishing a lot more.

First, by policing U.S. capital markets with vigor and efficiency, President Trump is taking steps to insure that U.S. capital markets remain the most transparent, most vibrant and most reliable in the world.

Second, bitcoin and other cryptocurrency investors are merely ascribing to the historically proven *greater fool theory*, betting that there will always be a "greater fool" in the cryptocurrency marketplace poised to pay a price based on higher valuation for an already overvalued bitcoin. Bitcoin and other cryptocurrency's anarchistic valuations remain generally unregulated and without any meaningful oversight, leaving them easily susceptible to fraud and chicanery by insiders, management and better-informed traders and market participants.

While ascribing to the greater fool theory might be a flawed and idiotic investment strategy, it has historically been a phenomenon that primarily impacts those who engage in it. However, combine the greater fool theory with the criminalities of bitcoin and other cryptocurrencies and the result can be fatal. Indeed, given the criminalities associated with cryptocurrency's use, which are almost as egregious and disturbing as the criminalities associated with its valuations, President Trump is supporting the SEC's sacred mission of investor protection.

Finally, investor protection and keeping markets safe are noble, nonpartisan goals. President Trump's concerns are anti-crime, pro-investor and pro-free markets. That is why President Trump is in good company with his new found crypto-antipathy — Warren Buffett refers to bitcoin as "rat poison squared," while Bill Gates declares that "I would short bitcoin if there was an easy way to do it."

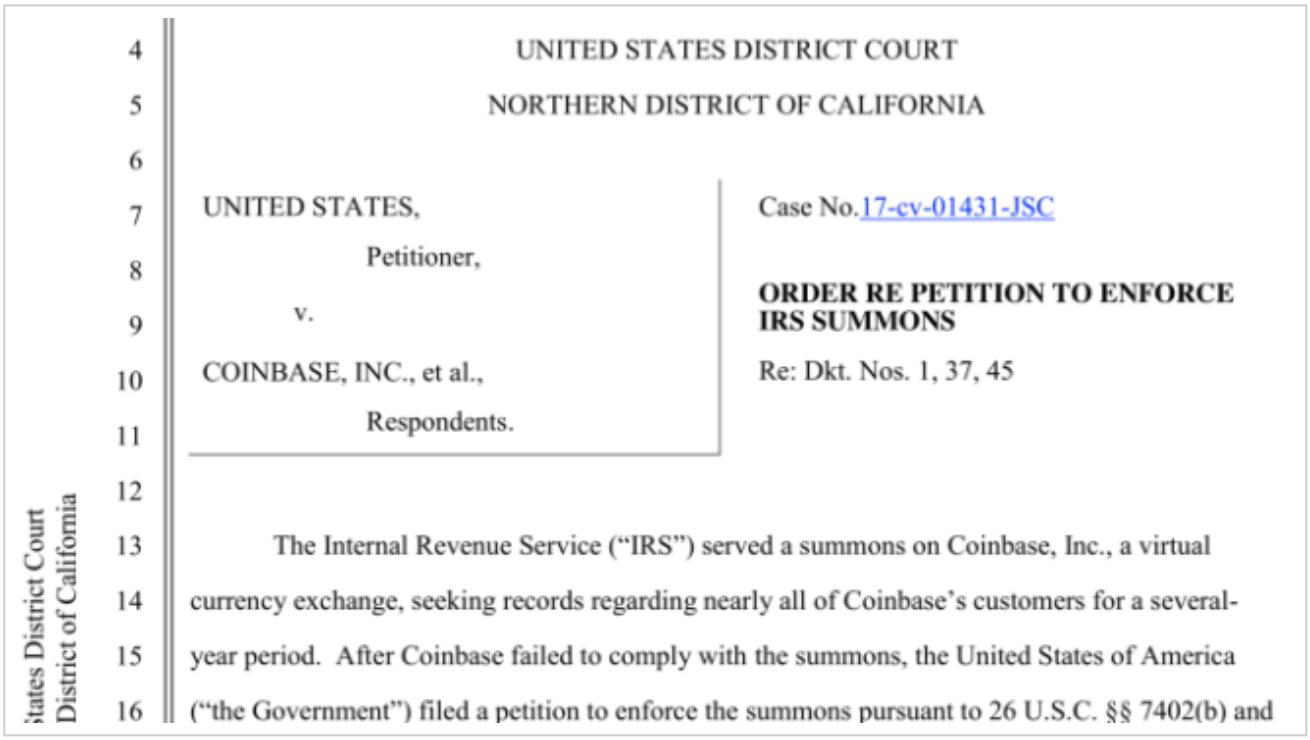
Unleash the IRS

In addition to the litany of financial regulatory agencies under his supervision, President Trump could also task an already crypto-active IRS to use gatekeeper theory to police crypto-related tax violations.

Cryptocurrency investors are typically extremely active traders and, for example, when a U.S. taxpayer has bought and sold bitcoin for a profit, a failure to pay the tax on that gain could be unlawful. According to a June 20, 2019 Bloomberg report, the IRS recently identified a slew of taxpayers who underreported their earnings from cryptocurrency income or completely failed to report such earnings, who should all expect to receive notices in the near future.

By issuing subpoenas to cryptocurrency platforms and other cryptocurrency gatekeepers regarding cryptocurrency transactions, the IRS can identify tax-delinquent U.S. taxpayers and disrupt the entire cryptocurrency marketplace. The IRS already engaged in this kind of investigation in late 2017 involving Coinbase about the transactions of over 14,000 users.

Coinbase was America's largest platform exchanging bitcoin into 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.



UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

UNITED STATES,

Petitioner,

v.

COINBASE, INC., et al.,

Respondents.

Case No. 17-cv-01431-JSC

ORDER RE PETITION TO ENFORCE IRS SUMMONS

Re: Dkt. Nos. 1, 37, 45

The Internal Revenue Service ("IRS") served a summons on Coinbase, Inc., a virtual currency exchange, seeking records regarding nearly all of Coinbase's customers for a several-year period. After Coinbase failed to comply with the summons, the United States of America ("the Government") filed a petition to enforce the summons pursuant to 26 U.S.C. §§ 7402(b) and

Coinbase refused to comply, resulting 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's reach. To read the judge's order, click here.

The Coinbase ruling clearly paved the way for a full scale IRS crypto-gatekeeper assault. According to Coindesk, a recent slide deck presentation from an IRS cyber training session details how the IRS is apparently already targeting companies associated with cryptocurrencies to identify tax cheats. The deck was apparently leaked on Twitter, and then Justin Cole, director of communication and education at the IRS criminal investigation unit, (astonishingly) confirmed to Coindesk that the deck was prepared by James Daniels, an IRS program manager for cybercrimes. Daniels apparently presented the deck to agency staff at an event at the World Bank in Washington, D.C., on June 5-7, 2019.

Per the leaked deck, the IRS is considering subpoenaing major tech companies like Apple, Google and Microsoft in search of taxpayers' unreported cryptocurrency holdings. Special Agent Daniels notes in the deck:

> *"Each application's function should be explored to determine whether or not the application can transmit, or otherwise allow, transactions in bitcoin . . . If so, it should be checked whether the app allows only peer-to-peer transactions, or also transactions with crypto-related businesses."*

The IRS is clearly off-and-running with what could become a creative and effective cryptocurrency sweep, which targets gatekeepers and seeks financial renumeration for taxes owed on crypto-transactions. President Trump could encourage more of the same, and not only impose hardships upon the cryptocurrency marketplace, but also increase the size of the U.S. Treasury at the same time.

The Road Ahead

President Trump's bitcoin blitzkrieg has already begun, led by none-other than Federal Reserve Chairman Jerome Powell. The Federal Reserve has created a working group to track the development of the cryptocurrency, and is working with central banks in other nations as well.

On July 10, 2019, at a congressional committee, just a day before the President's crypto-tweet-storm, Chairman Powell raised concerns about cryptocurrencies, especially Facebook's proposed Libra cryptocurrency, stating:

> *"Libra raises serious concerns regarding privacy, money laundering, consumer protection, financial stability . . . These are concerns that should be thoroughly and publicly addressed."*

The top Democrat on the Senate Banking Committee, Sherrod Brown of Ohio, echoed Chairman Powell's alarms, sending a July 10, 2019 letter on to Mr. Powell and others at the Federal Reserve, asking the central bank to protect consumers and the economy from "Facebook's Monopoly Money," stating:

> *"We cannot allow giant companies to assert their power over critical public infrastructure. The largest banks and the largest tech companies do not act in the interest of working Americans, but in the interest of themselves and their investors. The Fed must take a proactive role to ensure that the payments system remains accountable to the public."*

A few days later, on July 15, 2019, U.S. Treasury Secretary Steven Mnuchin joined the fray, stating that he had "very serious concerns" about cryptocurrencies going so far as to classify cryptocurrencies as "a national security threat" because of their use to fund illicit activities. Secretary Mnuchin explained:

> *"This is indeed a national security issue . . . Cryptocurrencies such as bitcoin have been exploited to support billions of dollars of illicit activity like cyber-crime, tax evasion, extortion, ransomware, illicit drugs, and human trafficking . . ."*

To me, the swarm of bitcoin and cryptocurrency is not a positive economic development. It is quite the opposite, and President Trump's anti-crypto sentiments are spot-on. Given its complete and utter lack of oversight and meaningful licensure, the cryptocurrency marketplace has spawned a growing global cadre of dangerous criminals. Bitcoin and other cryptocurrencies reside amid a libertarian financial realm of competing bandits. That is why, ironically, one of bitcoin's most useful criminal attributes is its use for the theft of other bitcoin.

Love him or hate him, President Trump's position against cryptocurrencies is not only groundbreaking, but also courageous. Cryptocurrency fanatics tout bitcoin and the like as items of inherent value (similar, for instance, to cash or gold) that are designed to enable purchases, sales and other financial transactions that will provide many of the same functions as long-established currencies such as the U.S. dollar, euro or Japanese yen. But, unlike so many others, President Trump is not fooled.

While one might appreciate cryptocurrency's appeal to individualism and reduced governmental meddling, the fact remains that cryptocurrencies are merely computer-generated chattel that operate as a remarkably effective and efficient criminal device. President Trump has joined his political enemies in combating bitcoin and other cryptocurrencies — and other government and private sector leaders should do the right thing and follow suit.

Just ask Baltimore, Florida, Dallas and the many other hospitals, municipalities and corporations who have paid ransomware demands over the past few years. To them, and to so many other victims, the mounting menace of cryptocurrency is not a matter of economic liberalism or financial freedom, it is a matter of life and death.

John Reed Stark is president of John Reed Stark Consulting LLC, a data breach response and digital compliance firm. Formerly, Mr. Stark served for almost 20 years in the Enforcement Division of the U.S. Securities and Exchange Commission, the last 11 of which as Chief of its Office of Internet Enforcement. He currently teaches a cyber-law course as a Senior Lecturing Fellow at Duke Law School. Mr. Stark also worked for 15 years as an Adjunct Professor of Law at the Georgetown University Law Center, where he taught several courses on the juxtaposition of law, technology and crime, and for five years as managing director of global data breach response firm, Stroz Friedberg, including three years heading its Washington, D.C. office. Mr. Stark is the author of "The Cybersecurity Due Diligence Handbook."