A Road Map For A Cryptocurrency Crackdown: Part 2

By **John Reed Stark** (August 2, 2019)

According to a recent Forbes article, companies now officially accepting cryptocurrencies include Starbucks Corp., Barnes & Noble Inc., Baskin-Robbins Inc., Bed Bath & Beyond Inc., Caribou Coffee Company Inc., Crate & Barrel, Express Inc., GameStop Corp., Jamba Inc., Lowe's Companies Inc., Nordstrom Inc., Office Depot Inc., Petco Animal Supplies Inc., Regal Cinemas Inc., Ulta Beauty Inc. and Amazon Inc.-owned Whole Foods Market Inc.

But none of these companies are admitting it.

That's right — none of these companies have independently confirmed they are accepting cryptocurrency. No announcements, no fanfare, no marketing. The silence is deafening. The reason why? Because for retailers, accepting cryptocurrency is extraordinarily risky, not just for the companies, not just for their customers, but for everyone.

Recently, in a late-evening and booming tweet storm, President Donald Trump lambasted cryptocurrencies, signaling for the first time significant presidential interest in eliminating them. Trump has clearly discerned how the cryptocurrency marketplace, with its utter lack of oversight and meaningful licensure, has spawned a growing global cadre of dangerous criminals who now pose a danger to U.S. citizens.

Part one of this three-part series **explored** how the president could direct the U.S. Department of Justice, the U.S. Department of the Treasury and its Financial Crimes Enforcement Network to initiate a sweep of the so-called gatekeepers and intermediaries of cryptocurrency transactions for violations of anti-money laundering, know-your-customer and other financial compliance requirements. Part one explained how, by focusing on the access points of cryptocurrency transactions, Trump can achieve fast, efficient and comprehensive results, cutting off cryptocurrency commerce at the throat.

Part two in this three-part series will discuss how Trump can apply the prosecutorial technique of gatekeeper theory: (1) to enforce wide-ranging and onerous state — and corresponding federal — money transmitter registration requirements pertaining to cryptocurrency financial intermediaries; (2) to prosecute cryptocurrency financial intermediaries that violate the Treasury Department's Office of Foreign Assets Control requirements; and (3) to subpoena any cryptocurrency financial intermediary to identify and prosecute possible tax cheats who failed to pay crypto-related capital gains tax.

Money Transmitter Registration

Trump 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 money service businesses, or MSBs, money transmitters are typically defined to include a person who "provides money transmission services, or any other person engaged in the transfer of funds." 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 Title 18 of U.S. Code Section 1960 covering the 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

On May 9, FinCEN published new guidance outlining how different companies, individuals and platforms in the cryptocurrency marketplace may be money transmitters under the Bank Secrecy Act and other relevant laws.

FinCEN's guidance provides a useful road map 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, operating in a highly suspicious and dangerous manner. According to FinCEN, owners and operators of 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;

- Peer-to-peer, or P2P, exchanges, which are software-operated, decentralized exchanges that facilitate individual buying and selling of cryptocurrencies. P2P could involve transferring one type of cryptocurrency for a different type of cryptocurrency, or exchanging cryptocurrency for other types of value. 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 [convertible virtual currencies] must comply with BSA regulations as a money transmitter;" and

- Decentralized distributed applications, or DApps, which are software programs that operate on a P2P network of computers running a blockchain platform, performing a variety of functions, including financial services. Generally, a DApp user pays a fee to the DApp 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)."

FinCEN filed its first **enforcement action** against a peer-to-peer cryptocurrency exchanger for breaking anti-money laundering rules on April 18, only a month before it issued the new guidance. The network 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, processing numerous suspicious transactions without ever filing a suspicious-activity report, taking steps to determine customer identity, or looking into whether funds were derived from illegal activity. For instance, Powers conducted: (1) more than 200 transactions involving the physical transfer of more than $10,000 in currency; and (2) more than 160 purchases of bitcoin for approximately $5 million through in-person cash transactions, with an individual identified through a bitcoin forum.

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."

Cryptocurrency and OFAC

Aside from anti-money laundering and know-your-customer requirements, OFAC also requires cryptocurrency financial intermediaries to conduct specific verification processes for offshore taxpayers.

OFAC administers and enforces economic and trade sanctions based on U.S. 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 U.S.

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.

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.

With respect to cryptocurrencies, OFAC recently released guidance, issued in the form of frequently asked questions, which explain that transactions involving cryptocurrencies will be treated the same as other transactions.

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."

Compliance with the economic sanctions programs administered by OFAC and in 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.

Unleash the IRS

In addition to the litany of financial regulatory agencies under Trump's supervision, the IRS could be tasked 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 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 delinquent U.S. taxpayers and disrupt the entire cryptocurrency marketplace. The IRS already engaged in this kind of investigation in late 2017 over the transactions of more than 14,000 Coinbase Inc. 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 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, 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 not outside the IRS's reach.

The Coinbase ruling 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, and presented on June 5-7. Per the leaked deck, the IRS is considering subpoenaing major tech companies like Apple Inc., Google Inc. and Microsoft Corp. in search of taxpayers' unreported cryptocurrency holdings.

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. Indeed, the IRS has already reportedly sent letters to more than 10,000 cryptocurrency holders, warning about penalties for failing to report income and pay tax on transactions involving virtual currencies. The IRS expects its mailing to be completed by the end of August. It is sending three variations of one letter, depending on the information it has about the recipient.

IRS Commissioner Charles Rettig said: "Taxpayers should take these letters very seriously. The IRS is expanding efforts involving virtual currency, including increased use of data analytics."

The third part of this series will discuss how Trump can similarly apply the prosecutorial technique of gatekeeper theory to cryptocurrency trading platforms, token custodians, digital wallets and other virtual financial intermediaries who violate broad and sweeping U.S. Securities and Exchange Commission statutes, rules and regulations. Part three also offers some thoughts going forward, because love him or hate him, Trump is spot on with his unqualified disdain for cryptocurrency.

John Reed Stark is president of John Reed Stark Consulting LLC. Stark served for almost 20 years in the Enforcement Division of the U.S. Securities and Exchange Commission, including 11 years as chief of its Office of Internet Enforcement.