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

Retailers Should Stay Away From Cryptocurrency

By **John Reed Stark** (June 13, 2019, 3:59 PM EDT)

John Reed Stark

Warren Buffett, perhaps the most celebrated investor ever known, refers to bitcoin as "rat poison squared." But bitcoin is worse than rat poison — it is more akin to the plague and mayhem that rats can spread if not properly contained.

Now, the bitcoin plague has spread to U.S. shopping malls. According to Fortune magazine, several big-name retailers, including Crate & Barrel, Nordstrom Inc. and Amazon.com Inc.-owned Whole Foods Market Inc., are planning to accept bitcoin and three other types of digital currency as part of a new initiative.

At first glance, creating cryptocurrency payment arrangements for retail products might seem like a no-brainer, falling squarely in line with classic, basic and critical marketing principles. Consider all the benefits:

- Sharing the excitement of cryptocurrency offers a unique chance to bond with tech-savvy customers, especially those beyond U.S. borders;

- By accepting cryptocurrency as payment, a retailer is demonstrating its commitment to creativity, modernization and originality — traits that even non-crypto-using customers might appreciate and find compelling;

- Payment flexibility can attract business in and of itself: Given that accepting debit and credit cards online can make a retailer more appealing to current and potential customers, so too can accepting other forms of payment, including cryptocurrencies; and

- Retailers can demonstrate tangible support for a client's libertarian financial preferences, setting themselves apart from their competitors who remain content to observe the crypto revolution from the safety and shelter of the sidelines.

But retailers should ignore all of the Marketing 101 crypto-blather. Given its complete and utter lack of oversight and meaningful licensure, the cryptocurrency marketplace has spawned a growing global cadre of dangerous criminals, and the risks for retailers accepting cryptocurrency run a perilous gamut of legal, regulatory, financial, ethical and reputational dangers.

For retailers, accepting cryptocurrency from customers in today's crypto-manic environment is, despite all of the high-tech allure, just not worth it — and a glaring exemplar of commercial ignorance, opportunistic corporate pandering and, sadly, plain old-fashioned executive irresponsibility and avarice.

The Dark Side of Cryptocurrency

Retailers accepting cryptocurrency are entering a virtual and international den of thieves that create a slew of known (and unknown) risks, including helping to facilitate noxious money laundering transactions

known (and unknown) risks, including helping to facilitate noxious money laundering transactions.

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.

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. Consider ransomware, one of the more prominent criminal uses of bitcoin.

In its May 2019 Beazley Breach Insights Report, insurer Beazley Group claims 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. The size of demands is also growing: In Q1 2019, the average ransomware demand reported to Beazley was $224,871, an increase of 93% over the 2018 average of $116,324.

How do most corporate victims of ransomware attacks pay the ransoms demanded? With bitcoin, of course — it's fast, reliable, verifiable, subject to little regulation and virtually untraceable. 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. Once the ransomware attackers take possession of the bitcoin payment, it can now be laundered via the dark web — that is, until now.

Now, ransomware attackers might have a new and better money-laundering option: using ransomware proceeds to buy a pint of avocado ice cream at Whole Foods, a Nantucket rug at Crate & Barrel or a Zegna Quindici tie at Nordstrom.

Guilt by Association

By accepting, enabling and empowering the bitcoin marketplace, U.S. retailers align themselves with extraordinarily dangerous threats to U.S. democracy and safety — not the healthiest of business associations.

Theoretically, anyone with an internet connection and a digital wallet can be part of any cryptocurrency platform, initial coin offering or other crypto-related endeavor operating anywhere on the globe — which, of course, opens the door for those with criminal motives.

For example, in July, 2018, special counsel Robert Mueller indicted twelve Russian intelligence officials for allegedly attempting to influence U.S. elections in 2016. 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."

The same rationale of secrecy and pseudo-anonymity unfortunately applies to terrorism financing. For instance, the Palestinian military-political group Hamas, which the U.S. government deems a terrorist organization, may be using the Coinbase cryptocurrency exchange for fundraising. Similarly, in December 2017, a woman was arrested in New York for allegedly obtaining $62,000 in bitcoin to send to the Islamic State. Around the same time, an Islamic State-affiliated darknet site called Isdarat sought bitcoin contributions from supporters.

Retailers might argue that criminals can use cash just as easily as they can use cryptocurrencies to commit crimes. But that is simply not true. In the U.S., pursuant to the Bank Secrecy Act, cash transactions involving traditional financial firms — such as banks, brokers and dealers, and money service businesses — 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.

Given the technological innovations at financial institutions, moving or warehousing cash without detection and surveillance has become significantly challenging, while the global cryptocurrency marketplace remains notoriously lacking in anti-money laundering and know-your-customer compliance. Hence the reason for crypto's popularity with crooks. Why would a retailer want to be associated with this kind of nefarious international criminal activity?

Fraud and Manipulation Risks

By accepting cryptocurrency from customers, retailers are not only indirectly endorsing cryptocurrency's oft-manipulated and wholly unregulated farcical valuations, but they are also encouraging their customers do the same. One could even go so far as to argue that enabling retail customers to pay via bitcoin is a not-so-subtle endorsement of bitcoin — which seems irresponsible, to say the least.

There is no central issuer of bitcoins or other cryptocurrencies, nor a Federal Reserve of bitcoins monitoring and tracking transactions or controlling their value. Thus, it should come as no surprise that the criminality associated with cryptocurrency's use is almost as egregious as the criminality associated with its valuations. Bitcoin and other cryptocurrencies' 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.

Along these lines, researchers from the University of Texas found that manipulation in the cryptocurrency market is rampant, and much of the runup 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, another cryptocurrency, was used to buy bitcoin at key moments when it was declining, which helped "stabilize and manipulate" bitcoin's price.

Cryptocurrency Financial Intermediaries

Retailers might argue that they are not taking on any valuation risk with respect to cryptocurrency — instead, they are transferring that risk to a reliable and trustworthy financial institution to safeguard the cryptocurrency, convert the cryptocurrency upon demand and orchestrate the cryptocurrency transaction.

But where to find an experienced, respected and heavily capitalized U.S. financial institution to serve as a cryptocurrency financial intermediary? 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 typically:

- Are not registered with any federal government agency and have no 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;
- Are not regulated by any quasi-governmental agency such as the Financial Industry Regulatory Authority;
- Warehouse property such as bitcoin (which is not officially recognized as a currency), without being insured by any federal agency, such as the Federal Deposit Insurance Corporation;
- Do not have any federal accounting requirements with respect to their assets;
- Do not report their financial condition in any form of official SEC filing, such as an annual report or Form 10-K;
- Do not have any federal record-keeping requirements with respect to their operations, communications or

- Do not have any federal record-keeping requirements with respect to their operations, communications or any other aspect of their business;

- Would assert that they have no specific federal requirements regarding the pricing of any cryptocurrency trading transaction, the use by employees of their payment systems, or any federal anti-manipulation requirements; and

- Would assert that they do not have the same federal compliance systems or code of conduct requirements of traditional financial institutions such as banks, investment companies, brokerages and other financial firms, who spend millions of dollars every year on internal compliance infrastructure and customer-protection-related infrastructure.

Cryptocurrency Exchanges Are Not "Exchanges"

Retailers accepting bitcoin and other cryptocurrencies are indirectly relying upon the many so-called cryptocurrency exchanges operating today — which often reside outside of U.S. borders. While these cryptocurrency financial platforms often give the impression to investors that they are regulated by, or meet the regulatory standards of, national securities exchanges, and that their operations are accordingly transparent, reliable, trustworthy and legitimate, this is not true.

Although some of these platforms claim to use strict standards to pick only high-quality digital assets to trade, the SEC, the primary regulator of securities exchanges, 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.

For instance, the U.S. Department of Justice announced in April of 2019 that it had 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.

Also in April 2019, New York's 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 its reserves of tether — a so-called "stablecoin" 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 is unclear. According to the New York AG, 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."

Who You Gonna Call?

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.

This means that when a retailer has a problem with a cryptocurrency matter, there exists no established federal government watchdog overseeing cryptocurrency transactions. To exacerbate matters, typical cryptocurrency transactions are by definition irreversible — so there is no anti-fraud guarantee from a financial institution, and no reversing the charges if any dispute or problem arises.

And even if there existed a formal federal regulatory complaint filing structure, the pseudo-anonymous nature of virtual currencies, the ease of cross-border and interstate transport, and the lack of a formal banking edifice create enormous challenges for law enforcement in investigating and apprehending any individuals who use cryptocurrencies for illegal activities.

Like bitcoin consumers, bitcoin-accepting retailers will encounter significant challenges should any bitcoin or other cryptocurrency transaction experience any problem — yet another risk that seems to far outweigh the benefits of cryptocurrency transactions.

Cybersecurity Risk

Transacting in bitcoin for a retailer and its customers 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. 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 has 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 quiet basement, and the proceeds can then be laundered through various digital wallets — and now, some of their friendly neighborhood retailers.

Renowned security technologist Bruce Schneier 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.

Say It Ain't So, Whole Foods

Benevolently-branded Whole Foods seems the most incongruous of these purportedly crypto-friendly retailers. Loyal Whole Foods Market customers laud the company's commitment to minimally-processed products free of nitrates, harmful pesticides, artificial colors, antibiotics, hormones and genetically modified organisms. Whole Foods farmed seafood standards are the highest in the industry.

Several times a year, each Whole Foods holds "5% days," where 5% of that day's net sales goes to support local education, hospitals or non-profits. Whole Foods Market also sets an example in its use of wind power, solar power, company-wide recycling programs, green buildings for their stores, etc. Whole Foods markets their benevolence aggressively — and consumers love it.

But by accepting cryptocurrency, Whole Foods would be assisting in the growth of an increasingly sophisticated, dangerous and terrorist-minded legion of worldwide criminals — which, to me, seems far more menacing than the threats posed by, for example, genetically-modified seafood.

Looking Ahead

Bitcoin resides amid a libertarian financial realm of competing bandits. That is why, ironically, one of its most useful attributes is how easy it is to steal. Retailers should think twice before lending an aura of legitimacy to bitcoin and other cryptocurrencies, and consider carefully their role in supporting cryptocurrency growth and encouraging cryptocurrency use.

In the history of financial innovation, modernization and invention, there has always existed one constant: Whatever the product, criminals will attempt to exploit its application. Bitcoin dramatically illustrates this axiom. Yet despite the treacherous reality of bitcoin's predominant uses, retail apparently wants in. It would seem that retailers have become so desperate for market share that they will resort to enabling terrorism, extortion and fraud.

fraud.

It's not just that bitcoin-friendly retailers have given little consideration to the myriad of victims of crypto-funded ransomware and the like. Cryptocurrency's liquidity risk, price volatility, cybersecurity vulnerabilities, commission fees, use in money laundering, ethical problems, tax issues and more create a situation that could be unmanageable or even intolerable for a retailer's shareholders, partners, affiliates and other fiduciaries. This is not to mention that for the most part, the entire cryptocurrency system resides amid an unregulated, mysterious and sinister environment — a patently poor choice of virtual venue.

Cryptocurrencies purport to be items of inherent value (similar, for instance, to cash or gold) that are designed to enable purchases, sales and other financial transactions, and promise to provide many of the same functions as long-established currencies such as the U.S. dollar, euro or Japanese yen. But retailers should not be fooled.

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 — and Whole Foods, Nordstrom and Crate & Barrel should not agree to accept chattel from customers as consideration for their purchases. We are not living in the 1800s, and this is not Deadwood, South Dakota.

Don't get me wrong, the blockchain technology on which cryptocurrencies are based may turn out to be the most exciting, disruptive, transformative and efficiency-enhancing breakthrough since sliced bread. But aside from complex issues of privacy, security, ethics and simple practicality, blockchain technology remains embryonic, has yet to be proven and happens to reside amid an economic ecosystem rife with fraud, deceit, dishonesty and thievery. Bitcoin is arguably blockchain's most celebrated accomplishment, yet much of bitcoin's value, outside of mere speculation, is derived solely from its ability to facilitate criminal activity.

Moreover, just because some mythical engineer has discovered a potentially revolutionary manner to engage in and verify commercial transactions (e.g., replacing a traditional corporate entry recorded in an intermediary institution's centralized ledger with a virtual entry recorded on a blockchain's decentralized distributed ledger), it does not mean that criminals should be permitted to create their own form of currency to use to commit robbery, theft, extortion and even murder.

I can appreciate that bitcoin 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 more for an already overvalued bitcoin. But the inherent scourge of bitcoin is an altogether different story. For retailers, where reputation is so critical, the risks of somehow becoming ensnared by, or even merely associating with, the dark and seedy underbelly of cryptocurrency are considerable.

Judge Stanley Sporkin, director of the SEC Enforcement Division from 1974 to 1981, general counsel to the U.S. Central Intelligence Agency from 1981 to 1985 and U.S. district court judge for the District of Columbia from 1985 to 2000, put it best when he said, "When you lie down with dogs, you wake up with fleas." When it comes to bitcoin and other cryptocurrencies, the fintech lawyers advising retailers contemplating crypto-cash registers should take heed of Sporkin's enduring admonition. Fintech legal advice should be plain and simple: Bitcoin is a plague, so stay as far away from it as you can.

John Reed Stark is the 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 the chief of its Office of Internet Enforcement.