**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

# Why Lawyers Shouldn't Accept Fees In Cryptocurrency: Part 2

By **John Reed Stark** (June 14, 2018, 1:27 PM EDT)

John Reed Stark

Law firms are increasingly accepting cryptocurrency as payment for services. This might seem innovative and forward-thinking, but law firms should think twice about the notion, and consider the comprehensive analysis of this two-part series, which discusses the broad range of significant risks law firms will confront when concocting cryptocurrency fee agreements with their clients.

**Part one of this series** provided some background and then focused on the logistical and ethical issues law firms will encounter should they opt to accept cryptocurrency as fees.

Part two will now focus on the statutory, regulatory and reputational implications of accepting cryptocurrency and conclude with some final thoughts looking ahead.

**Cryptocurrency AML Concerns: Myriad and Expanding**

Given that cryptocurrency transactions are pseudo-anonymous, encrypted and decentralized by nature, virtual currencies offer a convenient method of transferring funds obtained from illegal activities without an audit trail. This makes it harder for any central authority or law enforcement agency to track transactions, and to identify the individuals behind any of them — triggering a litany of anti-money laundering concerns. From buying a fake ID or a bottle of opiates, to receiving a cache of credit card numbers or stolen identities, to collecting a ransomware payment demand or even funding terrorist-related activities, cryptocurrencies represent a pseudo-anonymous virtual currency, which has unfortunately evolved into the payment mechanism of choice for unlawful transactions.

Slowing the growth of this unlawful behavior is a notion that appeals not just to market participants, but also to the myriad victims of crypto-funded ransomware, terrorism, drug dealing and the like. The government, in particular the Financial Crimes Enforcement Network of the U.S Treasury Department, is acutely aware of the dark side of cryptocurrency use. Along those lines, newly appointed FinCEN Director Kenneth Blanco, a former U.S. Department of Justice AML expert, who has testified before Congress about the threat of virtual currencies, has dedicated increasing resources to FinCEN's cryptocurrency enforcement program.

**A Lawyer's AML Obligations**

Given a lawyer's role in society and inherent professional and other obligations and standards, lawyers must at all times act with integrity, uphold the rule of law and take care not to facilitate any criminal activity. Lawyers must remain especially vigilant of the threat of criminals seeking to misuse the legal profession in pursuit of money laundering, terrorist financing activities and other similar crimes. These AML obligations arise from both ethical obligations for attorneys (discussed in **part one**) and AML statutory responsibilities established all around the globe.

In the U.S., pursuant to the Bank Secrecy Act, transactions involving traditional financial firms, such as banks, brokers and dealers, and money service businesses (MSBs), are subject to strict

such as banks, brokers and dealers, and money service businesses (MSBs), are subject to strict federal and state AML laws and regulations aimed at detecting and reporting suspicious activity, including money laundering and terrorist financing, as well as securities fraud and market manipulation. Following this example, law firms can create their own internal compliance programs, especially in the area of cryptocurrency transactions.

Although U.S. lawyers are arguably not subject to specific AML requirements, despite frequently playing a key role in handling financial transactions on behalf of clients, many western countries, including the United Kingdom and France, have established AML reporting requirements relating to attorneys.

Indeed, in a December 2016 report, the Financial Action Task Force singled out a number of nonfinancial sectors in the U.S. for failing to fight against money laundering. The report criticized the U.S. legal industry for not having an adequate understanding of money laundering vulnerabilities and the need to implement appropriate controls to mitigate them. Among the priority actions highlighted in the report was a suggestion that the U.S. apply more AML obligations to lawyers.

Putting aside the debate over lawyers being subject to AML rules — a debate certain to evoke strong opinions, especially from criminal defense lawyers — U.S. lawyers already have every reason to avoid such pitfalls if only to safeguard their own reputations. The last thing an innocent individual attorney or law firm wants is to be linked to something as unsavory as having unwittingly facilitated some manner of financial crime.

By instituting certain fundamental AML programs, if only as a matter of simple self-regulation, law firms can protect themselves from an AML mishap. After all, only when equipped with timely and relevant due diligence can attorneys, within their own sound judgment, truly render competent legal advice about a transaction or course of conduct.

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, law firms would start by obtaining clearly identifiable information about a prospective client, and identifying any potential risks of association.

Here is where cryptocurrency transactions can create challenging hurdles. Theoretically, anyone with an Internet connection and a digital wallet can be part of a cryptocurrency platform, initial coin offering or other cryptocurrency financing endeavor — which, of course, opens the laundry room door for those with criminal motives.

**Accepting Payment from Cryptocurrency Exchanges**

FinCEN has taken an interest in cryptocurrency and issued guidance for cryptocurrency exchanges to prevent and report money laundering activities. While these guidelines might not apply to a law firm that simply receives payment in cryptocurrency, attorneys must be aware of the risks and only accept payment through exchanges that actively take steps to prevent money laundering. But how? Cryptocurrency exchanges have only just begun operating and their existence itself may be short-lived. Both the U.S Securities and Exchange Commission and the New York State Attorney General's Office have raised serious concerns about their operations.

The SEC has issued a strong warning that cryptocurrency trading platforms might need to register with the SEC and meet all of the SEC's strict registration, compliance, auditing and other extensive regulatory requirements. Meanwhile, the Investor Protection Bureau of the New York Office of the Attorney General launched its Virtual Markets Integrity Initiative, a fact-finding inquiry into the policies and practices of platforms used by consumers to trade cryptocurrencies.

As part of a broader effort to protect cryptocurrency investors and consumers, the New York Attorney General’s Office sent questionnaires to 13 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 regulators, enforcement agencies, investors and consumers.

**Law Firm Entanglement**

Law firms should be viewing AML compliance as a necessity rather than a burdensome suggestion. The legal industry has already begun to feel the impact of compliance-related requirements through new anti-bribery and anti-money laundering terms that have appeared in outside counsel guidelines, legal master service agreements, and law firm engagement letters. If only as an internal risk mitigation measure, law firms have already begun to adopt some of the financial industry's internal practices to protect against AML violations.

When involved with cryptocurrency trading and remittance, law firms face more than the risk of being perceived by clients as organizations that support money laundering practices. The mere association with cryptocurrency is a lightning rod for governmental skepticism, suspicion, inquiry and scrutiny.

Not surprisingly, the notion of terrorists and criminals being able to launder money anonymously has not escaped the attention of U.S. law enforcement agencies, which have vowed to crack down on the virtual currency exchanges that serve criminals, even those operating outside the United States. The DOJ, acting in cooperation with FinCEN, has become increasingly active in policing criminals exploiting cryptocurrencies, leveraging AML statutes and regulations as its preferred statutory prosecutorial weapon. Thus, law firms also risk becoming entangled in costly and distracting federal or state investigations (or even the prosecutions) of the attorneys involved.

For instance, AML rules and regulations could impact the law firm advising an initial coin offering or token trading platform indirectly to the extent it relies on the law firm to enhance its bona fides, or if a law firm is somehow involved with clearing, settlement, custody or any other function. This is already true with respect to SEC investigations, where SEC Chairman Jay Clayton has specifically stated that he is concerned about legal advice given to unlawfully operating cryptocurrency trading platforms and illicit initial coin offerings.

By becoming increasingly sophisticated at co-opting a cryptocurrency network to establish an AML jurisdictional nexus, FinCEN and DOJ have laid the groundwork to link and prosecute both the masterminds and the foot soldiers of rogue and unregistered crypto-financing institutions. This could include the lawyers who become entangled in the undertaking (for instance, lending their reputations to promote a cryptocurrency firm's operations and money laundering or perhaps even serving as an indirect testimonial of a cryptocurrency's success and global acceptance).

Director of the SEC Enforcement Division from 1974 to 1981, general counsel to the Central Intelligence Agency from 1981 to 1985, and U.S. District Judge for the District of Columbia from 1985 to 2000, famed Judge Stanley Sporkin put it best when he said, "When you lie down with dogs, you get fleas." When contemplating cryptocurrency fee paying agreements, law firms would bode well to heed Judge Sporkin's enduring admonition.

**Cryptocurrency OFAC Concerns: A Matter of Life and Death**

Aside from a deep due diligence process of a crypto-paying client, a law firm accepting cryptocurrency must also conduct other verification processes for offshore clients, such as those required by the U.S. Treasury's Office of Foreign Assets Control.

Every U.S. person and business (including lawyers and law firms) is required to avoid engaging in financial transactions with certain individuals, entities and countries that are subject to U.S. economic sanctions. Accordingly, when a law firm relationship triggers OFAC compliance, it is the firm's obligation to ensure that none of its clients are on the list of prohibited individuals or entities maintained by OFAC. Law firms also need to be sure that clients and other business partners are not based in countries subject to broader economic sanctions.

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

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

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

**Cryptocurrency Tax Implications: All-Encompassing**

When a law firm conducts a transaction in a foreign currency, there are special rules that govern how gains or losses from the exchange of foreign currency are handled for tax purposes. Many cryptocurrency users assumed that those rules would also apply to virtual currencies. But they were wrong. Per IRS guidance issued in March 2014, for federal tax purposes, virtual currencies should be treated as property and not foreign currency.

Specifically, this means that when acquiring cryptocurrency, a law firm is required to record the fair market value of the property, which is deemed the law firm's "basis" in the property. When the asset is later exchanged, if the fair market value has increased, then the law firm has a taxable gain. Thus, a law firm accepting cryptocurrency as payment must also establish an appropriate manner to manage the taxes associated with a cryptocurrency fee arrangement.

The law firm must meticulously track and record the basis of cryptocurrency transactions, which requires knowing the value of the cryptocurrency when received and when sent, an exceedingly onerous and almost impossible burden (which, if it were even possible, would require a costly high-tech solution to automate).

**Looking Ahead**

In the celebrated "John Wick" thriller films, John Wick, played by Keanu Reeves, is an international assassin whose day-to-day work requires staying at the Continental, a hotel that functions as neutral territory for hired cutthroats and notorious murderers. The Continental Hotel has its own form of currency in the form of uniquely branded gold coins. The gold coins have images and Latin phrases on both sides. On one side, at the top of the coin is the phrase Ens Causa Sui, or "Something generated within itself." On the reverse side is the phrase Ex Unitae Vires, or "Out of unity comes strength." Sound familiar?

All services in the Continental are paid by the coins, including specialized services like weapons and munitions supply (from the Continental's sommelier) or body armor (from the Continental's seamstress). All the criminals Wick encounters seem to accept the gold coins — which can pay off everything from a bar tab to an invoice from the outside contractors who Wick hires to dispose of the typically 20-30 bodies he leaves behind after a particularly action-packed altercation.

A few years ago, the Continental's coin-based fee arrangements may have seemed limited to Hollywood blockbusters — but the reality of a John Wick currency system is happening right in our midst. Only instead of Winston's exclusively minted gold coins, there has sprouted a broad range of cryptocurrencies mined on virtual servers, rather than forged in iron and fire.

Once U.S. companies began accepting cryptocurrency as payment, U.S. law firms began to follow suit. Given the potentially wide-reaching application of the underlying blockchain technology, the virtual public ledger upon which cryptocurrency transactions reside, cryptocurrencies may someday become commonplace in the legal profession. So why not be a pioneer rather than the last in line?

New York has even begun setting the stage for cryptocurrency transactions in commercial transactions. Specifically, New York's Department of Financial Services allows merchants to sell

goods and services using cryptocurrencies, by requiring a BitLicense for anyone engaged in the financial use of virtual currencies, such as holding or storing virtual currency on behalf of others. It's no wonder that advocates of accepting cryptocurrency payments have even gone so far as to argue that the risk of accepting cryptocurrency payments is no different from that of accepting foreign currencies.

But taking on all of the associated risk with cryptocurrency payment arrangements is not for the faint of heart — and when a client mandates a cryptocurrency fee arrangement, it may be time for a lawyer to push back.

Federal and state law enforcement and regulatory efforts pertaining to all things crypto have increased exponentially in the past year, and some cryptocurrency institutions that seem to be thriving at the moment might not even be doing business in the future. This cryptocurrency liquidity risk — in addition to risks associated with price volatility, cybersecurity, commission fees, AML requirements, OFAC procedures, ethical obligations, tax burdens, entanglement, and the list goes on — create a situation that could be unmanageable or even untenable for a law firm's shareholders or partners. Not to mention that for the most part, the entire cryptocurrency system resides amid an unregulated, mysterious and arguably sinister environment.

Moreover, for a law firm, where reputation is everything, the risks of somehow becoming ensnared or even merely associating with the dark and seedy underbelly of cryptocurrency, are considerable. As one Virginia bar ethics officer recently wrote, addressing the issue of bitcoin payments for lawyers (in a co-authored article): "The bulk of people we know regard bitcoins as 'shady money' and they may well regard lawyers accepting bitcoins as 'shady lawyers.'"[1]

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

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

One final important note perhaps most bothersome to me: When clients discourage payments in U.S. dollars and mandate that their law firm devise a cryptocurrency fee arrangement, it may also be a subtle indication of a lack of respect and appreciation for the skills, talents, expertise and trustworthiness of counsel.

An important lesson I have learned from having been air-dropped into many bet-the-company crisis situations is that when a client does not believe in the value proposition of counsel, then payment, billing and invoice disputes will inevitably arise down the road. The same notion holds true for cryptocurrency fee payment arrangements.

Stated more simply, for clients who truly appreciate the sage counsel of their attorney, the form of payment should never be a deal-breaker.

---

*John Reed Stark is the president of John Reed Stark Consulting LLC, a data breach response and digital compliance firm. Formerly, Stark served for almost 20 years in the Enforcement Division of*

*digital compliance firm. Formerly, Stark served for almost 20 years in the Enforcement Division of the U.S. Securities and Exchange Commission, including 11 years as the chief of its Office of Internet Enforcement. He is the author of "The Cybersecurity Due Diligence Handbook."*



[1] http://www.slaw.ca/2018/05/29/a-view-from-virginia-is-it-ethical-for-lawyers-to-accept-bitcoins-and-other-cryptocurrencies/

---