Scared of Your Clients' Involvement With Cryptocurrency?

May 04, 2021

Cryptocurrency, and its most-noted asset Bitcoin, has been breaking into the mainstream press. While most lawyers have heard terms like "blockchain" and probably even know a few people who have been deeply interested in the world of cryptocurrency, far more of us have at best a vague understanding of crypto markets and how crypto is acquired, traded and converted to everyday dollars (or fiat currency). Given that the price of a Bitcoin is up over750% since April 2020 and approximately $56,000 per coin at the time of writing, the incentive to pay attention has increased. What was once thought to be a solely a niche product is becoming more widely accepted, as evidenced by an recent article in *Forbes* estimating that 10% of stimulus funds, or $40 Billion, will be used to purchase Bitcoin.

Given this rapid expansion of interest and participation in cryptocurrency transactions, it's not a matter of whether you have an interest in crypto, think it's all a bizarre techno-bubble, the eventual replacement for fiat currency, or somewhere in between. The fact of the matter is your clients, and future clients, are more likely than ever to have a connection to this market, and a brief review of the headlines can make this prospect seem terrifying.

Federal Prosecutorial Activity

Type "Bitcoin" into the search bar on the United States Department of Justice website, and you come up with over 800 hits, a scan of which will be heartburn-inducing for criminal defense lawyers. "Money laundering," "child exploitation," "terrorist financing," "dark web," "narcotics," and "Ponzi scheme" are all terms you will encounter in the first few pages of results. Click through to the press releases of various arrests, prosecutions, and plea bargains, and it becomes clear that there are some criminal elements, particularly abroad, that have an affinity for using cryptocurrency in attempts to transact illicit business.

It is undeniable that early in the history of cryptocurrency, those looking to evade legal and compliance measures were attracted by the anonymity of crypto transactions, which did not require routing through traditional, highly-regulated financial institutions, such as banks and brokerages that have well-developed anti-money laundering (AML) and know-your-customer (KYC) programs, Office of Foreign Asset Control (OFAC) compliance units, and generate Suspicious Activity Reports (SARS) for the U.S. Treasury.

The situation today is more complicated. NFL players, corporate CEOs, and entertainers openly touting their most recent Bitcoin purchase on social media are clearly not looking for anonymity with respect to their Bitcoin or crypto transactions, and traditional financial institutions are presumably getting in on the crypto craze for

reasons other than terrorist financing or dark web narcotics purchases. From an enforcement and prosecution perspective, there is a still a working suspicion, if not a presumption, among some prosecutors and regulators that crypto transactions are suspect in and of themselves. "Really?" they think, "if this was on the up-and-up, why didn't this transaction go through the bank?" or "what's wrong with a wire transfer?"

> *It is undeniable that early in the history of cryptocurrency, those looking to evade legal and compliance measures were attracted by the anonymity of crypto transactions, which did not require routing through traditional, highly-regulated financial institutions, such as banks and brokerages that have well-developed anti-money laundering (AML) and know-your-customer (KYC) programs, Office of Foreign Asset Control (OFAC) compliance units, and generate Suspicious Activity Reports (SARS) for the U.S. Treasury.*
>
> *The situation today is more complicated.*

What Is the Government Worried About?

The traditional financial services industry is both a highly-regulated industry in its own right, but also a de facto partner of federal law enforcement, without which entire regulatory and enforcement regimes arguably become ineffective. For example, if I deposit $10,000 in cash in my checking account through a teller window, my bank will generate a SAR for the U.S. Department of Treasury noting that transaction. The transaction may or may not generate questions or enforcement activity, but the bank knows to be on heightened alert for large cash transactions and its own internal compliance systems will kick in to ask me questions, have me fill out forms, etc. Similarly, if I walk into my bank and want to wire a significant amount of money to Uzbekistan, I will be questioned about the transaction, all parties will be run through an OFAC database to ensure that parties barred from the U.S. financial system are not involved, and regardless of any actually illegality of transaction, the bank may decline to process it simply based on "risk."

These examples get to the core of the government's concern with certain crypto transactions and platforms. Financial services businesses behave the way they do because of the obligations imposed by the Bank Secrecy Act, 31 U.S.C. §§5311, et seq., and because they are Money Services Businesses and thus governed by certain reporting requirements. (See, 31 C.F.R. §1010.100(t)(3), (ff)). These laws and regulations, though financial in nature, exist to prevent money laundering of the proceeds of substantive crimes such as drug or gun running, human trafficking, or terrorism. In theory, if an illegal narcotics dealer walked to a bank with $100,000 in cash proceeds of drug transactions, the bank would let the government know about the cash deposit, questions would be asked, and the substantive crime of drug dealing thwarted. If the bank stayed silent, it would face legal trouble for violating its obligations under the BSA.

In this context, it is easy to see the government's concern with crypto transactions and platforms that evade this regulatory structure in its entirety for the purpose of facilitating criminal activity. It is also easy to understand the fear of government regulators regarding the development of an entirely new digital currency or asset class that doesn't fit well within existing systems.

How Does This Apply to My Clients?

Happily, it need not. The "Wild West" aspect of crypto, particularly in the United States, is being reined in and plenty of legitimate avenues exist for the curious to try their hand in the crypto market. At this point many major U.S.-based platforms established to buy, sell, or trade Bitcoin and other crypto assets in a "digital wallet"

have registered as "money services businesses," have full "Know Your Customer" protocols and other compliance you are familiar with from your bank, and file SARS with Treasury as a bank would. Thus, if your client's interest is in acquiring some Bitcoin and seeing if it goes up another 750% this year, there are plenty of options to do so legitimately (granted, tax and other obligations remain, and a tax lawyer would need to be consulted regarding recognition of gains, etc).

Of course, not every client may be of the "buy and hold" variety. What if your client has a more active transactional relationship with crypto? Is that a sign of trouble?

> *At this point many major U.S.-based platforms established to buy, sell, or trade Bitcoin and other crypto assets in a "digital wallet" have registered as "money services businesses," have full "Know Your Customer" protocols and other compliance you are familiar with from your bank, and file SARS with Treasury as a bank would.*

Some Legitimate Business Cases for Using Crypto

Beyond novelty or "value store" uses of Bitcoin or other cryptocurrencies, there are increasing legitimate transactional uses of cryptocurrencies, particularly in the international arena. For example, in some populations, crypto can be a more efficient way for small dollar, and possibly even unbanked, users to handle remittances from the U.S. to a home country. Some businesses now "trade" payment of local invoices (in local currency) for Bitcoin on EBay-like platforms as an alternative to wire transfers for cross-border transactions. Bitcoin, though volatile, can also be a store of value in countries where hyper-inflation is an issue. This list is not meant to be exhaustive, but simply to note that, contra the view of some, mere involvement in cross-border crypto transactions is not a clear sign of money laundering or other illicit activity.

Just as with a "buy and hold" client, for legitimate users there are plenty of legitimate options in the U.S. that are registered with the appropriate authorities and can help facilitate various crypto transactions. Of course, they will require traditional KYC documentation and will keep records of the transactions that will be available to authorities. As always, if the client is reluctant to use these options because of these requirements, ask why.

Where Is the Trouble?

The forgoing should put most lawyers at ease about their clients' crypto activities. So where are the "parade of horribles" on DOJ's website originating? It is valuable to review the categories of cases that have created headlines, as doing so makes it relatively clear that market makers, trading platforms, and peer to peer networks — that is, specialized business that should be getting their own specialized advice, rather than random market participants — are the targets of enforcement actions.

Here are some categories of crypto cases that make the point:

Transactions/Business Models That Have Created Problems

1. **Not licensed as a money transmitter.** Kais Mohammad, a/k/a "Superman29," pled guilty to federal criminal charges that he operated an unlicensed money transmission business through a network of Bitcoin ATM-type kiosks. Mohammad, a former bank employee, intentionally failed to register his company with the U.S. Treasury Department's Financil Crimes Enforcement Network (FinCEN). Likewise, Kenneth Rhule, a resident of Washington State, was charged with conducting an unlicensed money transmitting business. Operating under the moniker "Gimacut93," Rhule advertised in-person cash-for-

Bitcoin exchanges on a website. Rhule offered to sell bitcoin at the fiat exchange rate, and would accept a variety of payments including unregistered VISA or Mastercard prepaid cards and other gift cards.

2. **Failure to take KYC AML precautions can lead to money laundering allegations.** The indictments of once-popular crypto exchanges BTC-e and Liberty Reserve and their operators stemmed in large part from a blatant disregard of KYC and AML requirements. In both cases, the indictments alleged that, since inception, the exchanges failed to implement basic BSA/AML controls and policies. Users were not required to even provide a name to open an account; only a user name, password, and email address were required.

3. **"Facilitation" of illegal activity — substantive charge.** Of course, actively working to facilitate crimes will result in a visit with law enforcement. In the cases of BTC-e and Liberty Reserve, discussed above, the indictments alleged that the operators purposefully designed the exchanges to help launder the proceeds of known criminal activity. While not an exchange, Dark Web site Backpage was targeted for accepting cryptocurrency from customers who publishing advertisements for "adult" and "escort" services. In addition, RG Coins and its operators were indicted for auction fraud, where false advertisements were posted online with the intent to defraud victims and launder money.

4. **"Mixing" — attempting to complicate the blockchain record and hide sources of money.** Mixing is a process by which an individual Bitcoin can be "washed" to hide its origin. Larry Harmon and his company Helix were charged with conspiracy to launder monetary instruments due in large part to Helix's mixing activity. In total, Helix exchanged over 354,000 bitcoins valued at approximately $311 million dollars.

5. **Traditional fraud — "pump and dump" of nontraditional coins.** Cryptocurrency presents fraudsters with ample opportunity to defraud unknowing investors, and the DOJ has taken a deep interest in these scams. BitClub serves as a prime example. The "BitClub Network" solicited money from investors in exchange for shares of pooled investments in cryptocurrency mining that rewarded existing investors for recruiting new investors. As a result, BitClub's operators were charged with knowingly and intentionally conspiring to devise a scheme to defraud and to obtain money and property from victims by false pretenses.

The Bottom Line

The crypto age is upon us. Even if you don't care or understand much about it, some of your clients will. Although regulatory clarity is well behind traditional financial services, there are plenty of legitimate players in the market at this point, as the U.S. regulatory regime has adapted. If your client for some reason wants out of that regime, ask yourself why and make sure you are comfortable with the reasoning. The ultimate risk is that anonymity or other irregular aspects to a transaction result in your client having facilitated a serious crime or participated in money laundering activity. As discussed above, however, for typical users, particularly new entrants to the crypto world, there are plenty of legitimate and legally safe platforms to dip your toe into the crypto waters.

Related people

Robert N. Driscoll