CorporateLiveWire

FRAUD & WHITE COLLAR CRIME 2019

EXPERT GUIDE

www.corporatelivewire.com

33 CHANCERY LANE

NYMAN GIBSON MIRALIS

Simmons & Simmons

NAVIGANT

Alma Angotti
United Kingdom | United States

alma.angotti@navigant.com
UK: +44 (0) 20 7550 4604 | US: +1 202 481 8398
www.navigant.com

Elizabeth Sisul
United States

elizabeth.sisul@navigant.com
+1 646 227 4725
www.navigant.com

Brandy Schindler
United States

brandy.schindler@navigant.com
+1 646 227 4881
www.navigant.com

Key Considerations and Risk Management Practices in Building Cryptocurrency Compliance Programs

By Alma Angotti, Elizabeth Sisul & Brandy Schindler

Cryptocurrency has quickly evolved from an instrument of the black market to an industry all its own. Cryptocurrency market participants still include bad actors, but now also include established financial institutions and startup organisations seeking to disrupt the financial services sector. While financial institutions often maintain robust Bank Secrecy Act/Anti-Money Laundering ("BSA/AML") and Office of Foreign Asset Control ("OFAC") Compliance Programs, startup organisations frequently lack the expertise and funding to do the same. Across both entity types, exposure to cryptocurrencies presents unique money laundering, sanctions, and regulatory risks that must be considered as the organisation modifies or builds an effective BSA/AML and OFAC Compliance Program.

This article will discuss key risk considerations for organisations that have exposure to the cryptocurrency industry. In addition, it will present risk management best practices for organisations that are amending or building a BSA/AML and OFAC Compliance Program that effectively addresses those risks.

Key Risk Considerations

This section presents key cryptocurrency risk considerations. It is not intended to be a comprehensive list, but rather a broad introduction to a selection of the more unique risks associated with cryptocurrencies.

The ability to trace transactions on the blockchain allows for the identification of the originating cryptocurrency wallet address and the beneficiary cryptocurrency wallet address. Bitcoin is said to offer "pseudo-anonymity" because it is often difficult to connect the cryptocurrency wallet addresses with real-world individuals and entities.

1. Money Laundering Risks

I. Pseudo-anonymity/Anonymity

Many erroneously believe that the most popular cryptocurrencies, including bitcoin, offer complete anonymity to its users. In reality, bitcoin transactions can be traced on the bitcoin blockchain. The ability to trace transactions on the blockchain allows for the identification of the originating cryptocurrency wallet address and the beneficiary cryptocurrency wallet address. Bitcoin is said to offer "pseudo-anonymity" because it is often difficult to connect the cryptocurrency wallet addresses with real-world individuals and entities. More concerning, and discussed later in this section, some blockchains now facilitate completely anonymous cryptocurrency transactions. Pseudo-anonymity and anonymity are attractive features to bad actors and may be especially useful during the placement[1] stage of money laundering, because it can obscure the source of the unlawful proceeds.

II. Cross-border transactions

Cryptocurrency transactions are executed online, and cross-border transactions require no additional effort from what is required for a domestic transaction. In addition, cryptocurrency users can store private keys[2] in many ways, including: as a Quick Response ("QR") code, in cold-storage wallets, or simply written down on a piece of paper. This gives a cryptocurrency user the ability to move private keys across borders with a piece of paper in his or her pocket, or by handing off that piece of paper to a co-conspirator crossing a border.

The ability to easily move money across borders facilitates the layering[3] stage of money laundering. Bad actors may leverage the ability to conduct cross-border transactions in order to direct complex transactions through multiple countries and/or through countries with weak regulatory frameworks. In addition, the inability to limit or control cross-border transactions makes it difficult for organisations and law enforcement to monitor transactions by jurisdiction.

Lastly, cryptocurrency can be safer from government seizure if a user's private keys are held in cold storage.[4] If a private key is stored on a piece of paper in your pocket, the government would have to find it in order to obtain access to the funds. Depending on the jurisdiction, authorities may also seek a court order requiring disclosure of the private key.[5,6,7]

III. Privacy-focused cryptocurrencies and mechanisms

As mentioned above, new cryptocurrencies have been developed to provide more privacy than what is offered by pseudo-anonymous cryptocurrencies. Listed in the table on the next page are examples of some of the most popular privacy-focused cryptocurrencies.

Cryptocurrency	Privacy Offered
Monero[8]	Hides sending address, receiving address, and transaction amount
Dash[9]	Automatically mixes coins before completing a transaction
Verge[10]	Obscures IP addresses using The Onion Router ("Tor")
Zcash[11]	Uses zero-knowledge proofs to encrypt sending address, receiving address, and transaction amount

In addition, mechanisms have been developed to provide cryptocurrency users with additional privacy irrespective of the cryptocurrency being used. Cryptocurrency mixers receive cryptocurrencies from multiple wallet addresses and store them in one wallet address. At this point, cryptocurrencies from an illegal source of income may be commingled with cryptocurrencies from a legitimate source of income. Next, the mixer redistributes the commingled cryptocurrencies into a new set of different wallet addresses, making it difficult to differentiate the "dirty" cryptocurrencies from the "clean" ones.

2. Sanctions Risk

I. Interest from sanctioned jurisdictions

Many countries are beginning to explore the potential application of cryptocurrencies and blockchain technologies to complement the existing international financial system. Other countries are exploring the potential application of cryptocurrencies and blockchain technologies to evade U.S. sanctions. Below is a brief description of how the governments and/or citizens of Iran, Venezuela, and Russia are leveraging cryptocurrencies to evade U.S. sanctions.

Iran

In November 2018, OFAC sanctioned two Iranian cryptocurrency exchangers.[12] The two individuals added to the OFAC list, Mohammad Ghorbaniyan and Ali Khorashadizadeh, were responsible for exchanging the proceeds of a ransomware attack into Iranian rials and depositing the rials into Iranian banks. To facilitate the exchange, the two individuals processed over 7,000 transactions through two cryptocurrency addresses. The Financial Crimes Enforcement Network ("FinCEN") issued guidance[13] that includes information about Iran's use of cryptocurrencies and in particular its use in evading sanctions. The guidance notes Iranians can access cryptocurrencies through exchanges based inside and outside of Iran, as well as through peer-to-peer exchangers.

Venezuela

In 2018, the government of Venezuela created a state-sponsored cryptocurrency called the "Petro." The Petro was launched on 20 February 2018, in response to the 25 August 2017, U.S. executive order[14] that prohibited transactions in Venezuelan new debt. On 19 March 2018, the U.S. issued an executive order[15] prohibiting transactions related to, the provision of financing for, and other dealings in the Petro.

Russia

In 2018, Time magazine published a report[16] asserting that the Venezuelan Petro was a collaboration between Russia and Venezuela. On 11 March 2019, the U.S. Department of the Treasury designated Evrofinance Mosnarbank. In the associated press release,[17] the Department of the Treasury noted that Evrofinance Mosnarbank is jointly owned by Russian and Venezuelan state-owned companies and that "Evrofinance emerged as the primary international financial institution willing to finance the Petro." The press release goes on to state that "[e]arly investors in the Petro were invited to buy the cryptocurrency by wiring funds to a Venezuelan government account at Evrofinance."

II. Screening cryptocurrency addresses

As mentioned previously, in November 2018, OFAC sanctioned two Iranian cryptocurrency exchangers. In its announcement, OFAC listed cryptocurrency addresses as identifiers. The cryptocurrency addresses are bolded and underlined below.

GHORBANIYAN, Mohammad (a.k.a. GHORBANIAN, Mohammad; a.k.a. "EnExchanger"; a.k.a. "Ensaniyat"; a.k.a. "Ensaniyat_Exchanger"), Iran; DOB 09 Mar 1987; POB Tehran, Iran; nationality Iran; Website www.enexchanger.com; Email Address EnExchanger@gmail.com; alt. Email Address Ensaniyat1365@gmail.com; Additional Sanctions Information - Subject to Secondary Sanctions; Gender Male; Digital Currency Address - XBT **1AjZPMsnmpdK2Rv9KQNfMurTXinscVro9V**; Identification Number 008-046347-9 (Iran); Birth Certificate Number 32270 (Iran) (individual) [CYBER2].

KHORASHADIZADEH, Ali (a.k.a. "Iranvisacart"; a.k.a. "Mastercartaria"), Iran; DOB 21 Sep 1979; POB Tehran, Iran; nationality Iran; Email Address iranvisacart@yahoo.com; alt. Email Address mastercartaria@yahoo.com; alt. Email Address alikhorashadi@yahoo.com; alt. Email Address toppglasses@gmail.com; alt. Email Address iranian_boy5@yahoo.com; Additional Sanctions Information - Subject to Secondary Sanctions; Gender Male; Digital Currency Address - XBT **149w62rY42aZBox8fGcmqNsXUzSStKeq8C**; Passport T14553558 (Iran) issued 28 Oct 2008 expires 29 Oct 2013 (individual) [CYBER2].

The cryptocurrency address is a string of alphanumeric characters. Traditional sanctions filters may be unable to alert on possible matches to cryptocurrency addresses. Therefore, a key risk consideration for organisations is how to effectively and efficiently screen transactions for this new type of sanctions indicia.

3. Regulatory Risk

In the U.S., it is fairly clear when an entity must be registered as a money services business ("MSB") or broker-dealer. The chart below reflects common cryptocurrency industry participants, and the U.S. regulatory frameworks that potentially apply to them.

In other jurisdictions, it is often difficult to identify the registration requirements associated with an organisation's business model. In addition, regulation related to cryptocurrencies continues to evolve. On 21 June 2019, the Financial Action Task Force ("FATF") adopted and issued an Interpretive Note to Recommendation 15.[22] The Interpretive Note "further clarifies the FATF's previous amendments to the international Standards relating to virtual assets and describes how countries and obliged entities must comply with the relevant FATF Recommendations to prevent the misuse of virtual assets for money laundering and terrorist financing and the financing of proliferation."[23]

Regardless of regulatory status, it is imperative that organisations maintain adequate risk management policies and procedures, especially related to BSA/AML and OFAC requirements. A lack of proper risk management, by either an established financial institution or a startup, may be unacceptable to regulators, or investors, given the risks associated with cryptocurrencies.

Miners	Do not have to register as an MSB unless mining cryptocurrency to sell or trade or on behalf of a third party.[18]
Cryptocurrency Exchanges	Must register as an MSB with the FinCEN if it operates in the U.S., which subjects it to certain requirements, including an AML program and record-keeping and reporting requirements. Also subject to state licensing requirements; exchanges doing business in New York may have to hold a BitLicense with the New York State Department of Financial Services.[19]
Securities, Futures, and Commodities	Companies offering cryptocurrency securities must register with the SEC as broker-dealers, unless they are exempt because they are considered an alternative trading system, and must comply with the associated rules, including the Customer Protection Rule. [20] Cryptocurrencies can also be considered commodities and therefore subject to regulation by the Commodity Futures Trading Commission ("CFTC"). [21]
All	All U.S. persons, or persons conducting business in the U.S., must comply with OFAC sanctions. The IRS treats virtual currency as property for federal tax purposes; all principles applicable to property transactions apply to transactions using virtual currency.

Risk Management

A BSA/AML and OFAC Compliance Program should be tailored to the risks of the organisation. This section describes strategies to identify and manage cryptocurrency risks as part of an organisation's overall BSA/AML and OFAC Compliance Program.

1. Risk Assessment

A Risk Assessment is the basis of an effective BSA/AML and OFAC Compliance Program, regardless of the size or business model of an organisation. The Risk Assessment should identify the inherent risks associated with the business and must include typologies and risk scenarios that are specific to cryptocurrencies. On 9 May 2019, FinCEN published an "*Advisory on Illicit Activity Involving Convertible Virtual Currency*."[24] This advisory contains a list of red-flag indicators of the abuse of virtual currencies and may be used as a basis for identifying inherent risks applicable to an institution. Once the inherent risks are identified, a catalogue of current and future controls should be established in order to calculate the residual risk to the institution. Once the organisation understands its risks and controls, an action plan should be put into place to remediate any gaps that are deemed unacceptable based on the risk appetite of the institution.

2. Know Your Customer/Customer Due Diligence

Given the pseudo-anonymity and anonymity characteristics of cryptocurrencies, it is imperative that organisations establish and maintain a robust Know Your Customer/Customer Due Diligence program. Organisations that offer exchange services are often the gateway between cryptocurrencies involved in illicit activities and fiat currency. In order to adequately identify a customer or counterparty involved in cryptocurrency transactions, it may be necessary to collect information specific to cryptocurrency use. Examples of this type of information includes, but is not limited to, the following:

- Cryptocurrency wallet addresses
- Expected cryptocurrency activity
- Identification of expected counterparties

3. Transaction Monitoring

Organisations can apply specialised tools and analysis to detect red flags in cryptocurrency transactions. A blockchain explorer is essentially a browser for the blockchain and can search the blockchain similarly to how users can search the internet. Blockchain explorers are limited to platforms related to a particular type of cryptocurrency. In other words, a user can use an explorer to search the Bitcoin blockchain or the Ethereum blockchain, but not both at the same time. The open-source, public nature of some blockchains allows for transparency from the point at which a cryptocurrency is created or mined, through each transaction in which the cryptocurrency is involved. Therefore, once a cryptocurrency wallet can be associated with a bad actor, the bad actor's transaction history can be viewed through the blockchain explorer.

Commercially available blockchain tracing software or connector tracking offers investigators researching a blockchain transaction the ability to trace the source and route of cryptocurrencies. These companies can often link or tag cryptocurrency wallet addresses that have confirmed ties to criminal activity.

4. Training

Institutions should regularly conduct training related to the risks associated with cryptocurrencies. It is imperative that all lines of defence understand the red flags associated with illicit cryptocurrency activity as well as how the organisation's policies and procedures attempt to mitigate those risks.

Conclusion

Cryptocurrencies present new and exciting opportunities for the financial system, but with those opportunities come additional risks. Employees at all levels must be responsible for ensuring that cryptocurrencies are not used to launder the proceeds of illicit activity or to evade sanctions through their organisation. Regulators are becoming increasingly more diligent in monitoring that organisations are meeting this obligation.

Adequate risk management practices can help an organisation to manage the risks associated with cryptocurrencies. A BSA/AML and OFAC Compliance Program is not one-size-fits-all; it must be tailored to the particular risks of an institution. However, it is imperative that all organisations strive to build an effective and robust program.

1. The placement stage of money laundering refers to the step wherein the launderer introduces illegally obtained funds into the financial system.
2. In simplified terms, private keys are used as the signature required to initiate a cryptocurrency transaction. More information may be found here: https://bitcoin.org/en/vocabulary#private-key.
3. The layering stage of money laundering refers to the step wherein the launderer conducts a series of transactions to distance himself or herself from the original source of the illegally obtained funds.
4. Cold storage refers to a cryptocurrency wallet that is not connected to the internet.
5. Christopher Williams, "UK jails schizophrenic for refusal to decrypt files," The Register, November 24, 2009, https://www.theregister.co.uk/2009/11/24/ripa_jfl/.
6. Declan Mccullagh, "Judge orders defendant to decrypt PGP-protected laptop," CNET, February 26, 2009, https://www.cnet.com/news/judge-orders-defendant-to-decrypt-pap-protected-laptop/.
7. Jon Matonis, "Key Disclosure Laws Can Be Used To Confiscate Bitcoin Assets," Forbes, September 12, 2012, https://www.forbes.com/sites/jonmatonis/2012/09/12/key-disclosure-laws-can-be-used-to-confiscate-bitcoin-assets/#42c171bcef54.
8. Monero, https://www.getmonero.org/ (last visited: February 24, 2019).
9. Dash, https://www.dash.org/ (last visited: February 24, 2019).
10. Verge, https://vergecurrency.com/ (last visited: February 24, 2019).
11. Zcash, https://z.cash/ (last visited: February 24, 2019).
12. U.S. Department of the Treasury Press Release, "Treasury Designates Iran-Based Financial Facilitators of Malicious Cyber Activity and for the First Time Identifies Associated Digital Currency Addresses," November 28, 2018, https://home.treasury.gov/news/press-releases/sm556.
13. U.S. Treasury FinCEN Advisory, "FIN-2018-A006: Advisory on the Iranian Regime's Illicit and Malign Activities and Attempts to Exploit the Financial System," October 11, 2018, https://www.fincen.gov/sites/default/files/advisory/2018-10-11/Iran%20Advisory%20FINAL%20508.pdf.
14. White House Executive Order, "Presidential Executive Order on Imposing Sanctions with Respect to the Situation in Venezuela," August 25, 2017, https://www.whitehouse.gov/presidential-actions/presidential-executive-order-imposing-sanctions-respect-situation-venezuela/.
15. White House Executive Order, "Executive Order on Taking Additional Steps to Address the Situation in Venezuela," March 19, 2018, https://www.whitehouse.gov/presidential-actions/executive-order-taking-additional-steps-address-situation-venezuela/.
16. Simon Shuster, "Exclusive: Russia Secretly Helped Venezuela Launch a Cryptocurrency to Evade U.S. Sanctions," Time, March 20, 2018, http://time.com/5206835/exclusive-russia-petro-venezuela-cryptocurrency/.
17. U.S. Department of the Treasury Press Release, "Treasury Sanctions Russia-based Bank Attempting to Circumvent U.S. Sanctions on Venezuela," March 11, 2019, https://home.treasury.gov/news/press-releases/sm622.
18. Financial Crimes Enforcement Network, "Application of FinCEN's Regulations to Virtual Currency Mining Operations," FIN-2014-R001, January 30, 2014, https://www.fincen.gov/sites/default/files/shared/FIN-2014-R001.pdf.
19. N.Y. Comp. Codes R. & Regs. tit. 23, pt. 200 (2015), https://govt.westlaw.com/nycrr/Browse/Home/NewYork/NewYorkCodesRulesandRegulations?guid=I7444ce80169611e594630000845b8d3e&originationContext=documenttoc&transitionType=Default&contextData=(sc.Default).
20. U.S. Securities and Exchange Commission and Financial Industry Regulatory Authority, "Joint Staff Statement on Broker-Dealer Custody of Digital Asset Securities," July 8, 2019, https://www.sec.gov/news/public-statement/joint-staff-statement-broker-dealer-custody-digital-asset-securities.
21. U.S. District Court, Eastern District of New York, CFTC v. McDonnell, et al., No. 18-cv-361, E.D.N.Y. March 6, 2018, https://www.cftc.gov/sites/default/files/idc/groups/public/@lrenforcementactions/documents/legalpleading/enfcoindroporder030618.pdf.
22. Financial Action Task Force, "Public Statement on Virtual Assets and Related Providers," June 21, 2019, https://www.fatf-gafi.org/publications/fatfrecommendations/documents/public-statement-virtual-assets.html.
23. FATF, "Public Statement on Virtual Assets and Related Providers."
24. Financial Crimes Enforcement Network, "Advisory on Illicit Activity Involving Convertible Virtual Currency," FIN-2019-A003, May 9, 2019, https://www.fincen.gov/resources/advisories/fincen-advisory-fin-2019-a003.