Miller & Chevalier

FRA

BRIEFING NOTE

TO: American Bar Association – Rule of Law Initiative

FROM: MILLER & CHEVALIER CHARTERED
Daniel Wendt, Daniel Solomon, James Tillen, Facundo Galeano

FORENSIC RISK ALLIANCE
Meredith Fitzpatrick, Peter Bott

DATE: August 28, 2023

RE: How Cryptocurrency Affects Current Transnational Anti-Corruption and Related Anti-Money Laundering Enforcement Efforts

I. EXECUTIVE SUMMARY

Miller & Chevalier Chartered and Forensic Risk Alliance jointly present this introductory briefing note on issues regarding anti-corruption enforcement and cryptocurrency to the American Bar Association's Rule of Law Initiative.[1] International anti-corruption enforcement efforts began with the passage of the U.S. Foreign Corrupt Practices Act ("FCPA") in 1977. Momentum developed in the 1990s and early 2000s with efforts to build international consensus on the topics in the United Nations and the Organization for Economic Co-operation and Development, followed by a surge of enforcement by U.S. regulatory authorities. Now, many countries around the globe have both new or revised legal regimes for prosecuting international corruption schemes as well as resources and political will for doing so. The legal regimes include both anti-corruption laws that may target either the giver or recipient of a bribe – including obligations for companies to maintain accurate books and records (as in the United States) or maintain a compliance program to prevent corruption (as in the United Kingdom) – as well as anti-money laundering laws that apply to those persons or entities involved in facilitating related transactions. These enforcement actions demonstrate that corruption often relies on surreptitious or covert transactions, involving third party intermediaries incorporated in jurisdictions with little or no transparency, often using banking systems that prioritize privacy over transparency.

Cryptocurrency, with its potential for private transactions of significant sums outside of the traditional banking networks, appears to present a potential challenge to the current anti-corruption and anti-money laundering enforcement efforts. Since its inception in 2008, cryptocurrency and blockchain technology has rapidly expanded both in adoption and complexity. Bitcoin is now a familiar term to most,

[1] This briefing note does not constitute legal advice, and in particular the references to legal regimes outside the United States are for background and context only.

but the realm of cryptocurrency now includes multiple types of blockchains, token types, financial services, non-fungible digital assets, and smart contracts. Entities wishing to launder illicit funds have also taken advantage of this new technology. In general, the current legal regimes against corruption and money laundering do not need revision or expansion to include transactions using cryptocurrency. Instead, the primary challenge is whether enforcement agencies or others (for example, companies conducting internal investigations) can detect the transactions and recover any ill-gotten gains once the transactions occur. While the notion that cryptocurrency is anonymous has largely been debunked by this point, a sophisticated actor may still use different aspects of the cryptocurrency ecosystem to effectively launder and conceal illicit funds.

II. BACKGROUND ON INTERNATIONAL ANTI-CORRUPTION ENFORCEMENT

A. Introduction to the Current U.S. and International Anti-Corruption Legal Framework

Bribery and secrecy go hand in hand, and the various legal regimes introduced to prevent bribery have typically required transparent transactions, when feasible. The global international anti-corruption legal regimes started in the United States when the federal government enacted the U.S. Foreign Corrupt Practices Act (FCPA) in 1977.[2] The legislation followed post-Watergate investigations into secret corporate political donations that revealed payments to foreign officials on a massive scale using offshore accounts. The FCPA had a two-prong approach to fight bribery: (i) the anti-bribery provisions, which generally apply to all U.S. persons and entities (and non-U.S. entities with sufficient nexus to the United States) and prohibit bribing foreign government officials; and (ii) the accounting provisions, which include requirements and prohibitions applicable to “Issuers”, i.e., companies registered on any U.S. securities exchange (regardless of the company’s location), and which ensure that transactions are authorized and accurately recorded. The U.S. Department of Justice (DOJ) and U.S. Securities and Exchange Commission (SEC) are primarily responsible for enforcing the law.

With regard to any potential bribes paid using cryptocurrency, it is important to note that the statute prohibits transactions using “anything of value” as long the transaction otherwise meets the statutory elements.[3] In other words, it does not matter if a bribe is paid using cash, wire transfers of fiat currency, gifts, free travel, or cryptocurrency. As described in the DOJ and SEC *FCPA Resource Guide*,[4] after hundreds of FCPA enforcement actions, this concept of “anything of value” has become broader and includes not only cash but many other types of benefits, including – as confirmed by recent charges against Sam Bankman-Fried, as noted later – cryptocurrencies.

Regarding the accounting provisions, the FCPA requires Issuers to: (a) maintain books and records accurately, fairly and in sufficient detail to reflect transactions and disbursements of the company’s assets; and (b) devise and maintain a system of internal accounting controls that ensures transactions are executed in accordance with management’s authorization. In other words, the FCPA not only prohibits

[2] The Foreign Corrupt Practices Act of 1977, as amended, 15 U.S.C. §§ 78dd-1, et seq. For more resources, see the DOJ website on the FCPA: https://www.justice.gov/criminal-fraud/foreign-corrupt-practices-act.

[3] *Id.* For example, *see* 15 U.S.C. § 78dd-1(a).

[4] *See* the FCPA Resource Guide and additional guidance here: https://www.justice.gov/criminal-fraud/fcpa-resource-guide

bribery, but forces public companies or Issuers to pursue transparency and avoid transactions without clear information on the purpose and the beneficiaries.

It is also important to know that, under the FCPA, companies can face liability for the actions of its third parties through one of two theories of liability: (1) direct liability for payments made by third parties who are "agents" of the Issuer; and (2) liability for payments made by third parties who are not "agents" of the Issuer, but are engaged in connection with the Issuer's business operations, if there is sufficient knowledge, as defined under the statute (indirect liability). In part because of how the statutory knowledge standard is set, companies subject to the FCPA cannot look the other way, and public companies or Issuers must have controls in place when engaging with agents, intermediaries, and other third parties.

In the international sphere, the Organization for Economic Co-operation and Development (OECD) followed U.S. anti-corruption efforts by adopting on November 21, 1997, the Convention on Combating Bribery of Foreign Officials in International Business Transactions.[5] As stated in the Convention, the OECD Anti-Bribery Convention, as it is also called, criminalizes bribery of foreign public officials in international business transactions through the implementation of legally binding standards to be applied by its members and provides several measures to ensure the implementation and enforcement of those standards. The OECD is considered responsible for encouraging its 38 signatories to adopt these standards and show real, tangible enforcement efforts.[6] Article 1 of the OECD Anti-bribery Convention is similar to the FCPA text in that it requires each party to make it illegal for "any person intentionally to offer, promise or give any undue pecuniary or other advantage, whether directly or through intermediaries, to a foreign public official…" Thus, this language is also broad enough to cover transactions using cryptocurrency.

Following the OECD efforts, the United Nations negotiated the text of the United Nations Convention against Corruption (UNCAC), which was adopted by the United Nations General Assembly on 31 October 2003. The UNCAC is the only anti-corruption global instrument, and considered the most important, that is legally binding for its 140 signatories. The purposes of the UNCAC include combating corruption more efficiently and effectively, promoting international cooperation and technical assistance, and promoting integrity, accountability, and proper management of public property. The Convention defines and address corruption with various definitions, including bribery, trading in influence, abuse of functions, and various acts of corruption in the private sector.[7] Regarding bribery and improper payments to public officials, the UNCAC includes in its provision the notion of "anything of value," and considers the term broadly.

As detailed later, DOJ and SEC enforcement of the FCPA picked up significantly in the early 2000s after progress on the OECD Anti-Bribery Convention and the UNCAC, and these developments together

[5] *See* the text of the Convention on Combating Bribery of Foreign Public Officials in International Business Transactions and related documents here: https://www.oecd.org/daf/anti-bribery/oecd-anti-bribery-convention-booklet.pdf

[6] The OECD has a periodic monitoring process to its members on the implementation and enforcement of the Convention through its Working Group on Bribery. More information here: https://www.oecd.org/daf/anti-bribery/countrymonitoringoftheoecdanti-briberyconvention.htm

[7] *See* the text of the United Nations Against Corruption here: https://www.unodc.org/unodc/en/corruption/uncac.html

raised the profile of bribery schemes internationally, which in turn highlighted how many countries did not have adequate legal regimes for pursuing charges against surreptitious transnational bribery. Following a scandal in the United Kingdom regarding BAE Systems, when former Prime Minister Tony Blair initially decided not to pursue charges against the company for allegations of bribery related to contracts with the Kingdom of Saudi Arabia, there was an effort to revise and improve British transnational anti-corruption law. The U.K. Bribery Act (UKBA) entered into force on July 1, 2010. As stated in the U.K. Ministry of Justice Guidance[8], the Act contains two general offences covering the offering, promising, or giving of a bribe (active bribery) and the requesting, agreeing to receive, or accepting of a bribe (passive bribery), at sections 1 and 2 respectively. The law also addresses commercial bribery, through the creation of offences related to bribery of foreign officials and corporate liability for those companies that failed to prevent bribery. Also, and different from the FCPA, under the UKBA it is a full defense for a company to prove that, although a bribery took place, it had adequate procedure in place to prevent its employees or other persons associated with the company to pay a bribe. The UKBA applies to giving a "financial or other advantage to another person" and therefore clearly would include cryptocurrency transactions within its scope.[9]

In France, several French companies entered into large resolutions with the U.S. Department of Justice (for example, Technip in 2013, Total in 2013, and Alstom in 2014, all with financial resolutions of several hundred million dollars). The Alstom resolution in particular provoked public discussion in France that the U.S. government was using the FCPA as a tool for American interests, in part because General Electric acquired a substantial portion of Alstom's assets following the FCPA resolution. Following these developments, the French government passed the Transparency, Anti-Corruption and Economic Modernisation Act 2016-1691 of 9 December 2016 (known as *Sapin II* after France's Finance and Economy Minister, Michel Sapin, who championed the bill). The changes from previous legislation include increased jurisdiction for French authorities to prosecute offenses committed abroad, expanded jurisdictional reach, the creation of a new anti-corruption agency, an obligation that companies of a certain size adopt a compliance program, new whistleblower protections, and the introduction of a deferred prosecution agreement (DPA) mechanism.[10] *Sapin II* defined bribery broadly and appears to include any transactions involving cryptocurrency. By 2020, the French and British authorities would use these new laws (*Sapin II* and U.K. Bribery Act, respectively) to cooperate with the U.S. authorities and bring the largest coordinated anti-corruption resolutions against Airbus, for total combined fines of nearly $4 billion.

In Brazil, following nationwide protests initially precipitated by rising bus fares, the government enacted the Clean Company Act (CCA) (Lei Anticorrupção) in 2013. One of the major developments brought by the law was strict liability for those companies that commit certain misconduct, such as corruption. Some of the other Anti-Corruption Law's most important changes were the implementation of penalties (administrative fine up to 20% of the company's gross income) and the new leniency agreement instrument. After the passage of the CCA, Brazil witnessed Operation Lava Jato (or Operation

[8] *See* the U.K. Ministry of Guidance on the U.K. Bribery Act of 2010 here: https://www.justice.gov.uk/downloads/legislation/bribery-act-2010-guidance.pdf.

[9] *See* Section 1 of the UK Bribery Act, available at https://www.legislation.gov.uk/ukpga/2010/23/section/1.

[10] *See, e.g.*, Miller & Chevalier's publication here: https://www.millerchevalier.com/sites/default/files/publications/SapinII_Zandieh_Moushey_11-10-16.pdf.

Car Wash), a massive series of investigations into fraud, bribery and money laundering, centered on transactions with Petrobras (the state-owned oil company, also publicly listed in the United States) as well as the construction firm Odebrecht and its subsidiary Braskem. A new Decree regulating the CCA entered into force in 2022, promoted by the results of the experience accumulated by the Federal Executive in the application of the Act during the eight years of its validity.[11] Several important settlements in 2022 demonstrate the sophistication of Brazilian authorities and establishes Brazil as a leader in anti-corruption enforcement, often coordinating with prosecutors in North America, Western Europe, and elsewhere.[12]

B. Introduction to the U.S. and International Anti-Money Laundering Legal Framework

The U.S. anti-money laundering framework is comprised of several statutes and regulations, starting with Bank Secrecy Act (BSA),[13] which was first enacted in 1970 and has implemented the notable obligations to banks, and certain other financial institutions, to report cash transactions over $10,000; keep records of cash purchases of negotiable instruments; and to report suspicious activity that might signify money laundering, tax evasion, or other criminal activities.[14]

Enacted in 1986, the Money Laundering Control Act (MLCA) introduced federal criminal penalties for money laundering. The MLCA is contained in 18 U.S.C. § 1956 (Section 1956) and 18 U.S.C. § 1957 (Section 1957). While Section 1956 prohibits domestic and international money laundering transactions for the purposes of promoting specified unlawful activity, concealment, or evasion, Section 1957 broadly prohibits knowingly depositing, withdrawing, or transferring funds greater than $10,000 that are derived from specified unlawful activity through a financial institution.[15]

In 2001, to deter and punish terrorists acts in the U.S. and around the world, the U.S. government enacted the USA Patriot Act. According to the Financial Crimes Enforcement Network, the Patriot Act amended the BSA and the MLCA to: (i) strengthen U.S. measures to prevent, detect and prosecute international money laundering and financing of terrorism; (ii) subject to special scrutiny foreign jurisdictions, foreign financial institutions, and classes of international transactions or types of accounts that are susceptible to criminal abuse; (iii) require all appropriate elements of the financial services industry to report potential money laundering; and (iv) strengthen measures to prevent use of the U.S. financial system for personal gain by corrupt foreign officials and facilitate repatriation of stolen assets to the citizens of countries to whom such assets belong.[16]

More recently, to promote transparency and combat obscurity in the financial crime activities, the U.S. Congress passed the Anti-Money Laundering Act of 2020 (AMLA) on January 1, 2021. Among its

[11] *See, e.g.*, https://www.gov.br/corregedorias/pt-br/assuntos/painel-de-responsabilizacao/responsabilizacao-entes-privados/lei-anticorrupcao-1

[12] There are similar efforts in many other countries, where new laws have been passed and/or there are new efforts to enforce the existing laws.

[13] 12 U.S.C. 1829b, 12 U.S.C. 1951-1960, 31 U.S.C. 5311-5314, 5316-5336

[14] *See, e.g.*, https://www.fincen.gov/resources/statutes-and-regulations/bank-secrecy-act

[15] *See* https://www.congress.gov/bill/99th-congress/house-bill/5077#:~:text=Sets%20forth%20fines%20and%20penalties,derived%20property%3B%20or%20(3)

[16] *See*: https://www.fincen.gov/resources/statutes-regulations/usa-patriot-act

most significant objectives, AMLA contains provisions to: (i) establish new federal-level beneficial ownership disclosure and transparency requirements (through the establishment of a beneficial ownership registration database implemented by the Financial Crimes Enforcement Network (FinCEN), a bureau of the U.S. Department of the Treasury); (ii) expand the BSA's purpose and mandate a review of the AML/ Combating the Financing of Terrorism (CFT) regulatory framework; (iii) promote public-private partnership and engagement opportunities on AML/CFT matters; (iv) introduce new staffing options and programs to enhance AML/CFT expertise; (v) promote international cooperation on financial crime matters, while protecting financial intelligence from misuse; (vi) strengthen enforcement tools to deter money laundering and other forms of financial crime; (vii) invigorate BSA whistleblower provisions; and (viii) expand the BSA's regulatory scope to include businesses that provide services involving "value that substitutes for currency."[17]

The U.S. regulators have attempted to expand the current regulations to apply to companies that provide different crypto services. For example, FinCen has been issuing guidance since 2013 regarding how and whether the BSA may apply to transactions in cryptocurrency, noting that the BSA defines currency in a way that emphasizes attributes of Fiat currency. This guidance, for example, addresses when dealers in cryptocurrency are considered "Money Transmitters" and covered by the BSA.[18] The SEC has focused on whether crypto assets are considered securities thus requiring crypto services providers to comply with the U.S. Securities and Exchange Act and related laws. Similarly, the Commodity Future Trading Commission (CFTC) has brought enforcement actions under the view that cryptocurrencies are commodities, and the companies trading those virtual currencies fall within CFTC jurisdiction. Finally, some state regulators, like the New York State Department of Financial Services (DFS), are requiring that crypto currency providers implement robust AML programs.

The U.K. Anti-Money Laundering Legal Framework includes the Proceeds of Crime Act of 2002, which requires certain persons to "submit a Suspicious Activity Report to the National Crime Agency if they know or suspect that a person is engaged in, or attempting, money laundering."[19] These regulations apply to certain entities, such as banks, credit unions, and other companies that provide certain financial services (e.g., investment managers, consumer credit companies, financial advisors, etc.).

As stated by the U.K. Financial Conduct Authority (FCA), Cryptoasset businesses need to be registered in its agency under the Money Laundering, Terrorist Financing and Transfer of Funds Regulations of 2017 (MLRs) and comply with all the requirements and the regulations. This is the only way the Cryptoasset businesses can provide certain type of its services in the United Kingdom.[20]

In the international sphere, the Financial Action Task Force (FATF) is the inter-governance body established in 1989, and based in Paris, that sets international standards regarding prevention of money

[17] *See:* https://crsreports.congress.gov/product/pdf/R/R47255#:~:text=Among%20other%20provisions%2C%20AMLA%20also,monetary%20transactions%20(%C2%A76313).

[18] *See:* https://www.fincen.gov/resources/statutes-regulations/guidance/application-fincens-regulations-persons-administering; https://www.fincen.gov/sites/default/files/2019-05/FinCEN%20Guidance%20CVC%20FINAL%20508.pdf

[19] *See, e.g.*, https://www.fca.org.uk/firms/financial-crime/money-laundering-terrorist-financing

[20] *See:* https://www.fca.org.uk/firms/financial-crime/cryptoassets-aml-ctf-regime

laundering and terrorist financing.[21] The 39-member body sets international standards to ensure national authorities can effectively go after illicit funds linked to drugs trafficking, the illicit arms trade, cyber fraud and other serious crimes. The FATF established Standards for countries to implement to its internal legal framework in response to preventing organized crime, corruption and terrorism. Around 200 countries have committed to implement those Standards, which are given in the form of Recommendation for the countries to implement.[22] The FATF has established Standards for virtual assets and encourages countries to "fully and effectively implement" the standards.[23]

C. Brief Notes Regarding FCPA and AML Enforcement in the United States

We include as exhibits slides detail of the enforcement of the FCPA, showing the number of enforcement actions against natural persons and corporations since 2010, the ten largest resolutions under the FCPA, and the ten largest internationally-coordinated resolutions (which include an FCPA resolution).[24] In short, DOJ and SEC have actively enforced the FCPA against both corporations and individuals for nearly 20 years, often with very large financial resolutions involving the corporations. The DOJ and SEC are able to have an outsized role internationally for anti-corruption enforcement in part because (a) many foreign companies list shares on U.S. stock exchanges and therefore become subject to the FCPA; and (b) many problematic transactions are made in U.S. Dollars, which often creates connections to the United States (for example, through correspondent bank transactions). Statistics may vary, but it is fair to say that more than 90% of FCPA resolutions include surreptitious payments, whether payments via third parties (who often hide the nature of the transaction) or transfers of value through travel, gifts, or entertainment. For example, we include below a chart prepared by the Foreign Corrupt Practices Act Clearinghouse of the Stanford Law School (in collaboration with Sullivan & Cromwell), where it shows that out of a total of 324 FCPA matters since 1977, 290 resolutions/cases have involved third-party intermediaries (such as agents, consultants, or contractors).[25]

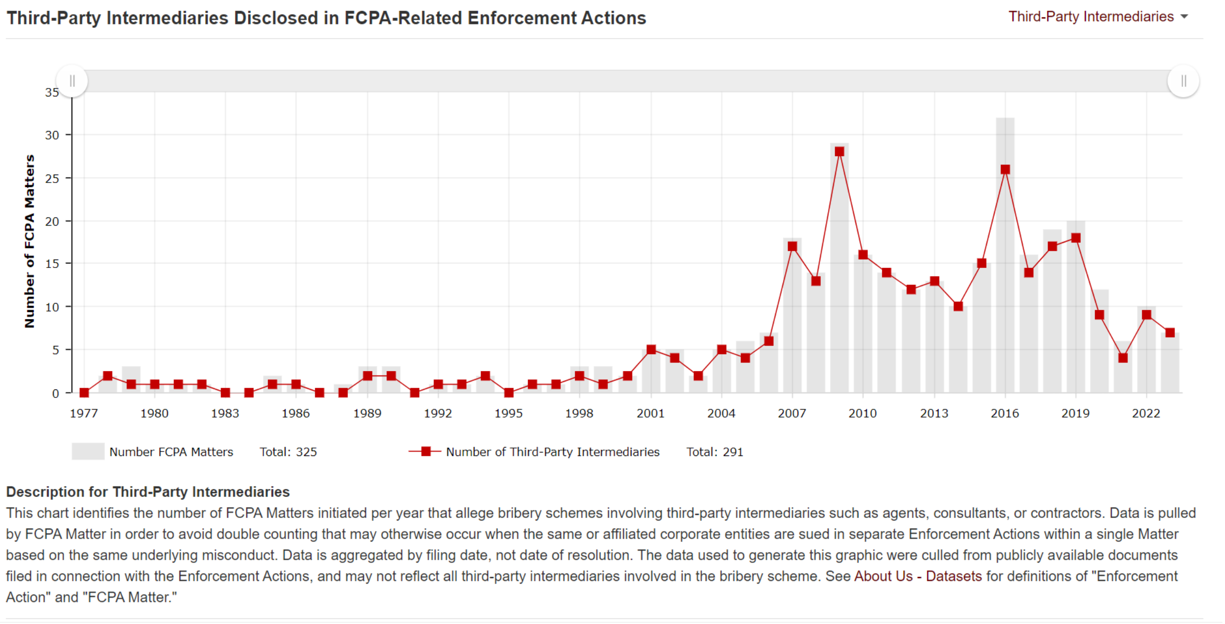
[21] For more information, see here: https://www.fatf-gafi.org/en/the-fatf/who-we-are.html

[22] *See* the FATF Recommendations here: https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Fatf-recommendations.html

[23] *See* https://www.fatf-gafi.org/en/topics/virtual-assets.html (last visited August 26, 2023).

[24] *See* Attachment A.

[25] *See:* https://fcpa.stanford.edu/statistics-analytics.html?tab=4



Third-Party Intermediaries Disclosed in FCPA-Related Enforcement Actions

Description for Third-Party Intermediaries

This chart identifies the number of FCPA Matters initiated per year that allege bribery schemes involving third-party intermediaries such as agents, consultants, or contractors. Data is pulled by FCPA Matter in order to avoid double counting that may otherwise occur when the same or affiliated corporate entities are sued in separate Enforcement Actions within a single Matter based on the same underlying misconduct. Data is aggregated by filing date, not date of resolution. The data used to generate this graphic were culled from publicly available documents filed in connection with the Enforcement Actions, and may not reflect all third-party intermediaries involved in the bribery scheme. See About Us - Datasets for definitions of "Enforcement Action" and "FCPA Matter."

In many cases, enforcement agencies follow transactions from companies subject to the FCPA into bank accounts controlled by third party intermediaries, who in turn transfer some or all the funds into bank accounts controlled by public officials (either directly or indirectly). In theory, third party intermediaries involved in making corrupt payments on behalf of corporate clients could consider whether cryptocurrency transactions present less enforcement risk than fiat currency transactions – because the transaction may be viewed as more private and less likely to be detected; and because there may be less risk of triggering jurisdiction under the FCPA (although both points depend on the specific facts in a transaction and may not be true for many transactions involving cryptocurrency).

The anti-money laundering rules are often used in anti-corruption cases against any intermediaries who transfer improper payments to public officials as well as against the public officials themselves. (The FCPA is not constructed to allow for prosecution of public officials themselves from receiving improper payments.) For example, the anti-money laundering rules were used in the following enforcement actions so far in 2023:

- On January 25, 2023, Jose Luis De Jongh Atencio (procurement Manager for Citgo, considered a government official) and Roberto Enrique Rincón Fernández (a U.S.-based businessman) were sentenced to prison for their participation in a corruption and money laundering scheme involving Petróleos de Venezuela (PDVSA), the Venezuelan state-owned oil company with a controlling stake in Citgo.

- On January 26, a grand jury indicted Venezuelan Supreme Court President and current Supreme Court Justice Maikel José Moreno Pérez on charges of conspiring to violate money laundering laws.

- On January 30, Saman Ahsani (former Chief Operating Officer of Monaco-based intermediary company Unaoil) was sentenced pursuant to an earlier plea agreement related to allegations of conspiracy to violate the FCPA, money laundering, and obstruction of justice.

- On March 3, Ng Chong Hwa, also known as Roger Ng (former Managing Director for Goldman Sachs) was sentenced to 10 years of imprisonment for various FCPA and related money laundering charges.
- On June 12, Alvaro Ledo Nass (a former government official in Venezuela, due to his employment at PDVSA) was sentenced to three years in prison for conspiracy to commit money laundering, following a plea agreement announced earlier this year.

These FCPA and money laundering enforcement actions often reveal schemes for secrecy regarding transactions, such as the following: (a) the use of shell companies in jurisdictions that maintain confidentiality of ownership; (b) routing payments through banking jurisdictions with lax anti-corruption and AML enforcement; (c) the use of surrogate ownership for companies; (d) the generation and use of false or misleading documentation to support transactions. As noted, digital assets or cryptocurrency potentially present a new tool for bad actors interested in secrecy and transferring bribes to corrupt public officials, with the potential to do so in a way that does not generate a trail revealing the true nature of the transaction. To date, we have identified only one known corruption-related charge in the United States – against Samuel Bankman-Fried (as summarized below) – in which digital assets were used as the vehicle for alleged bribes. It is unclear whether digital assets are in fact being used for corrupt payments, although enforcement activity in other areas does show the current use of cryptocurrency in illegal financial transactions.

III. BACKGROUND ON CRYPTOCURRENCY

A. Summary of Relevant History of Cryptocurrency

Though earlier iterations of cryptocurrencies were experimented with at the end of 20th century, cryptocurrency as we know it today first pierced the cultural zeitgeist with the October 2008 publication of Satoshi Nakamoto's whitepaper outlining the concept of Bitcoin. Just over two months later, the first Bitcoin software was released in January 2009.[26] Bitcoin is made possible through blockchain technology, a decentralized and distributed public ledger system. Networks of computers, referred to as nodes, work in unison to validate transactions to create an immutable and permanent accounting system on the blockchain. The term Bitcoin can refer to the cryptocurrency itself, or the blockchain, as Bitcoin is the native currency of the Bitcoin blockchain.

The Bitcoin blockchain has gone through several open-source protocol modifications, called hard forks, since its inception. A hard fork is a change in the protocol that makes older versions invalid and incompatible with the new version, thereby creating a split with a new blockchain and cryptocurrency. Notable Bitcoin hard forks occurred in 2014 with Bitcoin XT, 2016 with Bitcoin Classic and Bitcoin Unlimited, 2017 with Bitcoin Cash and Bitcoin Gold, and 2018 with Bitcoin SV.

A variety of cryptocurrencies have been created either as forks of Bitcoin, in the case of Litecoin, or as their own unique blockchain. Ethereum, the second largest blockchain, was introduced in a 2013 whitepaper by Vitalik Buterin, with the official launch coming two years later in 2015.[27] Ethereum and Bitcoin share many of the same concepts between the blockchains, but differ in several distinct technical

[26] *See:* https://archive.nytimes.com/www.nytimes.com/interactive/technology/bitcoin-timeline.html#/#time284_8155

[27] *See:* https://ethereum.org/en/history/

ways, chiefly in their transaction models. Bitcoin is an Unspent Transaction Output (UTXO) model, while Ethereum is an account-based model. Though these differences are technically complicated, they can be thought of as the difference between peer-to-peer cash transactions, in the case of Bitcoin, and bank account to bank account transactions, in the case of Ethereum, with Ethereum being an account debit and credit system.

Just as Bitcoin ushered in the modern era of cryptocurrency, Ethereum ushered in the modern era of smart contracts in the cryptocurrency space. Smart contracts, described in more detail below, are self-executing programs on the blockchain that execute a specific function defined by the contract.[28] These smart contracts permit more diverse items to exist and be transacted on the blockchain through the implementation of different protocols, with the ERC-20 and ERC-721 standards being the most notable on the Ethereum blockchain. The ERC-20 standard, proposed in late 2015, facilitates the existence of fungible tokens on the Ethereum blockchain through smart contracts by any entity with the programmatic know how. These tokens can be virtual representations of any fungible asset conceivable, with the more pronounced being stablecoins, a cryptocurrency pegged one to one to a fiat currency, such as Tether (USDT).[29] The ERC-721 standard, proposed in early 2018, facilitates the existence of non-fungible tokens ("NFTs") on the Ethereum blockchain. There are a variety of applications for the ERC-721 standard, though the most prominent can be colloquially referred to as digital collectibles.[30]

B. There Are Various Means for Converting Fiat Currency to Digital Currency or Otherwise Conducting Cryptocurrency Transactions, and the Level of Transparency Varies Significantly

Cryptocurrency can be used as its own currency, but it is more likely that bad actors using cryptocurrency to conduct an illegal transfer would acquire fiat currency, convert it to cryptocurrency, transfer the cryptocurrency to the control of a public official (or their surrogate), at which point the public official may transfer the cryptocurrency asset back into fiat currency or another tangible asset (real estate, luxury goods, etc.). As of 2023, the most common way to interact with the cryptocurrency ecosystem is through an on-ramp/ off-ramp, meaning a point of conversion between cryptocurrency and fiat currency. There are a variety of services known as Virtual Asset Service Providers (VASPs) that can facilitate the conversion of cash, bank account linked fiat currency, or funds from a money service business linked fiat currency account to a desired cryptocurrency.

VASPs commonly provide custodial wallets, meaning the private keys are in the custody of the VASP, and transactions are facilitated through that service. A non-custodial wallet is a wallet software or hardware in which the user of the wallet retains total control of the private keys, seed phrases, and activity of the wallet. Custodial wallets, like wallets managed by exchanges such as Coinbase, Binance, and Kraken, will typically require a collection of KYC information at some level, whereas non-custodial wallets inherently do not, like MetaMask, Elctrum, and Trezor.

The FATF defines a VASP, as business that conducts one or more of the following activities or operations for or on behalf of another natural or legal person: exchange between virtual assets and fiat

[28] *See:* https://ethereum.org/en/developers/docs/smart-contracts/#:~:text=Further%20reading-,What%20is%20a%20smart%20contract%3F,a%20type%20of%20Ethereum%20account

[29] *See:* https://ethereum.org/en/developers/docs/standards/tokens/erc-20/

[30] *See:* https://ethereum.org/en/developers/docs/standards/tokens/erc-721/

currencies; exchange between one or more forms of virtual assets; transfer of virtual assets; safekeeping and/or administration of virtual assets or instruments enabling control over virtual assets; or participation in and provision of financial services related to an issuer's offer and/or sale of a virtual asset.[31]

VASPs can take a variety of forms, such as peer-to-peer (P2P) marketplace, Over the Counter (OTC) Exchange, or Bitcoin ATMs. In P2P marketplaces users can transfer crypto directly between themselves without a centralized authority. These marketplaces match traders with one another and oftentimes have more lax compliance and reporting standards.[32] In OTC Exchanges, transactions occur in a closed environment between two individuals on a negotiated price outside of the market fluctuations.

Smart contracts are self-executing programs on the blockchain that execute a set of functions that automatically enforce a set of actions once a set of conditions are met, as defined by the contract. As opposed to externally owned accounts (EOA) addresses, or accounts controlled by individuals or entities, addresses generated by the smart account do not have an administering authority. They do not have private keys, and because they are self-executing, smart contracts enable users to affect the transfer of tokens without a middleman or authorizing party.[33]

Decentralized Finance (DeFi) products and services function by using smart contracts. DeFi encompasses loaning, lending, trading, saving, and purchasing that exists outside of centralized crypto VASPs. Within DeFi, Decentralized Exchanges, or DEXs facilitate crypto to crypto trades using smart contracts according to a predefined set of parameters and can facilitate enhanced anonymity of its users as they do not collect KYC information. DEXs like Uniswap do not support crypto to fiat conversions.

C. In Some Instances, Cryptocurrency Transactions Can Be Transparent or Traced, But There Are Also Options in the Market That Still Prevent Visibility Into the Nature of Any Transfer

A variety of tools and methodologies exist to read and interpret blockchain data in its raw, difficult to decipher state. Open-source utilities, such as block explorers, provide an elementary way to identify pertinent information in crypto transactions. Open-source block explorers provide the pseudonymous identifiers of the sending address, transaction hash, and the receiving address as well as the timestamp and amount of the transaction, allowing investigators to manually trace the flow of funds. Proprietary tools such as TRM Labs and Chainalysis deliver a more advanced, powerful way to conduct blockchain investigations and trace the flow of funds. These companies, created in the mid-2010s, provide software that facilitates cryptocurrency investigation by automating "clustering", a technique that groups wallet addresses reasonably believed to belong to the same entity, and access to proprietary databases that deanonymize pseudonymous cryptocurrency addresses on blockchain(s) when there is known attribution data. These software tools are used by leading cryptocurrency institutions, law enforcement agencies, regulators, investigative firms, and traditional financial institutions as a part of rigorous compliance programs, investigative projects, and a host of other business development operations.[34]

[31] *See*: https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Guidance-rba-virtual-assets-2021.html

[32] *See:* https://cointelegraph.com/news/what-is-p2p-trading-and-how-does-it-work-in-peer-to-peer-crypto-exchanges

[33] *See:* https://blog.chainalysis.com/reports/ofac-sanction-suex-september-2021/

[34] *See:* https://www.chainalysis.com/customer-stories/

Created to counteract the transparent nature of the blockchain, privacy coins, such as Monero and Zcash are coins with enhanced cryptography and privacy features that conceal the identity of and transaction history of their users. These currencies make it exceedingly difficult to trace with even the most advanced tools through transaction joining, stealth address creation, and cryptographic coding.[35]

Further complicating matters, cryptocurrency mixing services or tumblers enhance the anonymity of cryptocurrency transactions by combining transactions and funds with other pools of transactions or funds. Mixers can be either centralized, where a third party retains a pool of cryptocurrency and switches out denominations of currencies, or decentralized, in the case of CoinJoin transactions, which facilitate multiple users joining in a transaction to redistribute funds.

IV. RECENT ENFORCEMENT ANTI-CORRUPTION AND ANTI-MONEY LAUNDERING ENFORCEMENT ACTIONS INVOLVING CRYPTOCURRENCY

We summarize below various enforcement actions that relate to corruption and money laundering issues related to cryptocurrency. In January 2020, the U.S. Department of Treasury Office of the Comptroller of the Currency (OCC) issued a Consent Order against M.Y. Safra Bank, FSB (Safra), based in New York, New York. From November 2016 to February 2019, Safra began rolling out banking services for "digital asset customers," including digital currency ATM operators, crypto arbitrage trading accounts, blockchain developers and incubators, and traditional fiat currency money service business (MSB) customers. According to the Consent Order, Safra failed to implement commensurate controls to address the increased BSA/AML risk that came with this expanded, higher-risk customer base. Based on this alleged failure, the OCC found that Safra had violated regulations requiring certain BSA monitoring procedures. Under the Consent Order, Safra is required to adopt certain compliance commitments, including the establishment of a Compliance Committee, development of a written program of internal controls and processes to ensure compliance with suspicious activity report (SAR) filing requirements, development of a written program of internal controls for compliance with the BSA, development of a risk assessment that accounts for BSA/AML and Office of Foreign Assets Control (OFAC) risk.

On December 13, 2022, the DOJ charged Sam Bankman-Fried (SBF), founder and principal of cryptocurrency exchange company FTX Trading Ltd. (FTX) with an eight-count indictment.[36] In the indictment, SBF is accused of running "a wide-ranging scheme … to misappropriate billions of dollars of customer funds deposited with FTX … and misleading investors and leaders to FTX and Alameda Research, the cryptocurrency hedge fund also founded by SBF."[37] On March 27, 2023, the DOJ introduced a superseding indictment against SBF which introduced FCPA-related allegations focused on China.[38] The superseding indictment added one count of conspiracy to violate FCPA's anti-bribery provisions to a range

[35] *See:* https://blog.chainalysis.com/reports/privacy-coins-anonymity-enhanced-cryptocurrencies/#:~:text=Privacy%20coins%20are%20cryptocurrencies%20with,but%20within%20a%20digital%20ecosystem.

[36] *See:* https://www.justice.gov/usao-sdny/press-release/file/1557571/download

[37] *See* DOJ Press Release: FTX Founder Indicted for Fraud, Money Laundering, and Campaign Finance Offenses, *available at* https://www.justice.gov/opa/pr/ftx-founder-indicted-fraud-money-laundering-and-campaign-finance-offenses (last visited August 26, 2023).

[38] *See:* https://www.millerchevalier.com/sites/default/files/resources/FCPAReview/FCPASpringReview2023_SBF-Superseding-Indictment.pdf

of other fraud and other ranges linked to FTX's business and demise. According to the indictment, in "early 2021" Chinese authorities froze "cryptocurrency trading accounts" with a value of approximately $1 billion held by FTX's affiliated company, Alameda Research (Alameda), as part of an investigation. Bankman-Fried and others "acting at his direction" tried "numerous methods to unfreeze the [a]ccounts or otherwise to regain access to the cryptocurrency in the [a]ccounts" to no avail. The DOJ alleges that "after months of failed attempts to unfreeze the [a]ccounts," Bankman-Fried "agreed to and directed" "a bribe payment of cryptocurrency then worth approximately $40 million from Alameda's main trading account to a private cryptocurrency wallet" – at which time the Chinese Alameda accounts were unfrozen.

On January 18, 2023, the National Cryptocurrency Enforcement Team charged Anatoly Legkodymov, the founder and majority shareholder of Hong Kong-based crypto exchange Bitzlato, with conducting an unlicensed money transmitting business. U.S. authorities allege that key to Bizlato's branding was that it had "loose or non-existent" Know Your Customer (KYC) requirements. According to U.S. authorities, among other things, Bitzlato allegedly exchanged hundreds of millions of dollars with Hydra, a "darknet market" that facilitated the sale of contraband. U.S. authorities allege that Bitzlato knowingly serviced U.S. customers, conducted transactions with U.S.-based exchanges, was run using U.S. online infrastructure, and, for at least some time, was being managed by the defendant while he was in the U.S. Concurrently, and for the first time, FinCEN announced an Order pursuant to section 9714(a) of the Combating Russian Money Laundering Act identifying Bitzlato as a "primary money laundering concern," which prohibits certain fund transfers involving Bitzlato by covered financial institutions. Legkodymov is a Russian citizen who primarily resides in China but was arrested by U.S. authorities while in Miami.

On April 24, 2023, DOJ unsealed two indictments charging a North Korean Foreign Trade Bank (FTB) representative, Sim Hyon Sop (Sim), for his role in two money laundering conspiracies designed to financially benefit the DPRK, in violation of sanctions, by using cryptocurrency.[39] The first indictment alleges that Sim and three OTC traders conspired to launder funds stolen in cryptocurrency exchange hacks and make payments in U.S. dollars for goods through Hong Kong based front companies on behalf of the North Korean government. According to the indictment "As part of its global cyber intrusion campaign, North Korea's RGB cyber actors have targeted and conducted cyberattacks against virtual currency exchanges around the world to generate revenue for the regime".[40] To convert the stolen cryptocurrency for fiat currency, the actors then utilized an OTC trader to circumvent the KYC measures in place at most cryptocurrency exchanges. According to the UN Security Council's March 4, 2021 Report of the Panel of Experts, "the country [DPRK] continues to target over-the-counter virtual asset brokers, especially those located in China…peer-to-peer services and those that do not collect "know-your-client" information, including over-the-counter exchange services, present a growing target for Democratic People's Republic of Korea cyberactors".[41]

The second indictment involves DPRK's IT workers scheme. In this scheme, DPRK based workers obtain illegal employment in IT industries by applying for remote IT jobs and bypass background checks

[39] *See:* https://www.justice.gov/opa/pr/north-korean-foreign-trade-bank-representative-charged-crypto-laundering-conspiracies

[40] *See:* https://www.justice.gov/usao-dc/press-release/file/1581286/download

[41] *See:* https://documents-dds-ny.un.org/doc/UNDOC/GEN/N21/034/37/PDF/N2103437.pdf?OpenElement

with fraudulent identification documents and other obfuscation techniques. These workers then request payment for their work in cryptocurrency and send their earnings back to DPRK through a variety of methods, one of which being FTB representatives such as Sim. According to the indictment, from 2021 to March 2023, “SIM, and by extension North Korea’s FTB, received over $24 million dollars’ worth of laundered virtual currency, including at least $12 million from IT worker revenue generation, in violation of U.S. sanctions against North Korea”.[42]

OFAC also cited DPRK’s use of sophisticated cryptocurrency enabled money laundering techniques to evade sanctions in their enforcement actions against multiple cryptocurrency mixers. In May 2022, OFAC announced its first ever sanctions on a virtual currency mixer, Blender.io, which DPRK actors allegedly used to launder stolen cryptocurrency, to include cryptocurrency stolen by DPRK-sponsored hacking group Lazarus Group.[43] Following that announcement, in August 2022, OFAC sanctioned the cryptocurrency mixer Tornado Cash which was used to launder more than $7B worth of virtual currency since its creation in 2019, including over $455M stolen by the Lazarus Group.[44] OFAC’s sanctioning of Tornado Cash was significant as it was the first time a decentralized, non-custodial smart contract was targeted for sanctions, meaning a portion of the over 40 Ethereum wallet addresses sanctioned by OFAC are associated with code on the Ethereum blockchain, and not with an individual or group controlling Tornado Cash. OFAC’s willingness to establish precedent by sanctioning a smart contract signifies the severity of DPRK’s use of DeFi to obfuscate the source and destination of illicitly acquired funds for the purposes of evading sanctions.

V. NEW LEGISLATION PROPOSALS RELATED TO CRYPTOCURRENCY RISKS

As a result of the previous enforcement actions, Capitol Hill has recognized cryptocurrency’s place in the illicit financial crime ecosystem and has proposed several bills to prevent the US financial system from being used in cryptocurrency enabled crime. On July 19, 2023, a bipartisan group of Senators introduced legislation targeting money laundering and sanctions evasion using DeFi.[45] Under the proposed Crypto-Asset National Security Enhancement and Enforcement (CANSEE) Act, DeFi services will have to meet the same AML and sanctions compliance obligations as other financial companies, most notably the requirement to conduct due diligence on their customers and report suspicious transactions to FinCEN. The CANSEE act would also require Crypto ATMs to verify the identity of each counterparty in every transaction using a kiosk.

Additionally, in May 2023, Senator Elizabeth Warren stated that she would reintroduce the Digital Asset Anti-Money Laundering Act.[46] Originally introduced in December 2022 by Senators Warren and Roger Marshall, the proposed legislation aims to bring cryptocurrency into greater compliance with the

[42] *See:* https://www.justice.gov/usao-dc/press-release/file/1581281/download

[43] *See:* https://home.treasury.gov/news/press-releases/jy0768

[44] *See:* https://home.treasury.gov/news/press-releases/jy0916

[45] *See:* https://www.warner.senate.gov/public/index.cfm/pressreleases?ID=CDCD1854-DA84-4A11-B834-476E88308B70

[46] *See:* https://www.warren.senate.gov/newsroom/press-releases/at-hearing-warren-calls-for-closing-crypto-loopholes-fueling-fentanyl-trade

current AML/CFT rules that govern the fiat currency finance system.[47] In reintroducing the bill, Senator Warren highlighted crypto's roll in the fentanyl crisis. According to a May 2023 study by blockchain intelligence company Elliptic, China-based companies selling fentanyl precursors or fentanyl itself received millions of dollars in cryptocurrency.[48] In April 2023, OFAC sanctioned Chinese based individuals and businesses who were supplying fentanyl precursors to Mexican cartels for the production of fentanyl intended for the U.S. market.[49] Notably, the sanctions listed cryptocurrency wallets used by these businesses to receive customer payments.

VI. FORECAST ON ISSUES REGARDING ABC/AML REGIMES AND CRYPTOCURRENCY

A. Cryptocurrency Generally Does Not Offer More Secrecy or Privacy Compared to Offshore Accounts for Companies Incorporated in Low Transparency Jurisdictions

For the average user, cryptocurrency may offer less privacy compared to offshore accounts for companies incorporated in low transparency jurisdictions, as many blockchains leave behind a deep footprint of financial activity for those who know how to analyze it. As cryptocurrency enabled crime has evolved since the landmark Silk Road investigation, so has the ability of the United States Government (USG) to utilize open-source and commercial blockchain analysis tools to conduct robust on-chain investigations and determine the source and destination of cryptocurrency funds.

The most common and easiest way to on-ramp from fiat to cryptocurrency is through a VASP. Most VASPs collect robust KYC information and have sophisticated AML and transaction screening programs. This means that if an investigative body identifies that funds were transferred to a VASP, it is highly likely that personal identification information about the account holder would be available pursuant to the appropriate legal process. Additionally, it is typical that the higher the amount of funds flowing through an account at a VASP, the higher the scrutiny paid by the VASP's Financial Intelligence Unit (FIU) towards the source of funds and true identity of the account holder.

However, there are ways to convert fiat currency to cryptocurrency without using a VASP or mining it yourself. As discussed above, P2P and OTC exchanges connect buyers and sellers to affect a transaction and seldom require either party to verify their identity or the legitimacy of the source and destination of funds. There are also VASPs that tout that they do not collect KYC information. Bitcoin ATMs also provide an avenue to purchase bitcoin without KYC, but many Bitcoin ATMs have CCTVs that could capture the individual making the purchase.

To circumvent KYC procedures and blockchain analysis techniques, a user trying to conceal their identity could transfer cryptocurrency purchased via a P2P or OTC exchange to a privately held wallet. They could then move the funds through a series of DEXs and cryptocurrency mixers, creating an extraordinarily complicated flow of funds. This process is further complicated if the activity is conducted across blockchains, by using a DeFi powered cross-chain bridge or a centralized cryptocurrency swapping

[47] *See:* https://www.warren.senate.gov/newsroom/press-releases/warren-marshall-introduce-bipartisan-legislation-to-crack-down-on-cryptocurrency-money-laundering-financing-of-terrorists-and-rogue-nations

[48] *See:* https://www.elliptic.co/blog/chinese-businesses-fueling-the-fentanyl-epidemic-receive-millions-in-cryptocurrency-payments

[49] *See:* https://home.treasury.gov/news/press-releases/jy1413

service. Additionally, one could further obfuscate their trail converting a common cryptocurrency like bitcoin or Ethereum to a privacy coin like Monero or ZCash, then use a cryptocurrency swapping service to go back to bitcoin or another cryptocurrency.

The reverse is also true, in that if a user wanted to cash out anonymously, they could use one of the methods mentioned above to go from crypto to fiat currency. While the trail of the above activity would be visible on the blockchain, the who behind the transactions would be totally anonymous as the funds never pass through a party that collects KYC information. By using P2P/OTC exchanges in conjunction with cross-chain swaps, privacy coins, and cryptocurrency mixers, cryptocurrencies can offer a tremendous amount of privacy for a sophisticated cryptocurrency actor, even in the age of sophisticated blockchain analysis tools.

B. There Are Numerous Efforts to Seize and Reclaim Ill-Gotten Gains via Cryptocurrency (which also reduces the likelihood that crypto will be main tool of choice for corruption/money laundering)

In recent years, the USG has conducted several high-profile cryptocurrency seizures, which were accompanied by equally high-profile press releases. In June 2021, the DOJ seized $2.3M in cryptocurrency paid to the DarkSide ransomware variant.[50] Earlier that year, DarkSide famously struck the Colonial Pipeline with ransomware, resulting in fuel shortages and price increases. The seized funds allegedly represent the proceeds of the May 8, 2021 ransomware payment to DarkSide.

In November 2021, the DOJ announced the historic seizure of approximately 50,676.18 bitcoin, then valued at over $3.36B, in connection with Silk Road dark web fraud.[51] At the time, this was the largest cryptocurrency seizure in the history of the DOJ and the second largest financial seizure ever. That record was broken shortly after, when in February 2022 the DOJ announced the seizure of $3.36B in cryptocurrency directly linked to the 2016 hack of cryptocurrency exchange Bitfinex.[52] In her remarks, Deputy Attorney General Lisa O. Monaco stated that the arrest and seizure showed that "cryptocurrency is not a safe haven for criminals." These cases demonstrate how the USG has successfully utilized blockchain analysis in cryptocurrency investigations.

However, for funds to be seized, the subject's funds need to be held by a custodial exchange, meaning an exchange that holds a customer's assets and private keys, or the USG needs to acquire the subject's private key(s) through other means. This could happen by finding the key(s) through an authorized search of the subject's electronic devices or residence, or by the subject providing them to the government voluntarily in a custodial or non-custodial interview. For example, in the Bitfinex hack case, the USG executed search warrants on online accounts controlled by the subjects and obtained access to files that contained the private keys required to access the cryptocurrency wallet that directly received the stolen funds from Bifinex.

[50] *See:* https://www.justice.gov/opa/pr/department-justice-seizes-23-million-cryptocurrency-paid-ransomware-extortionists-darkside

[51] *See:* https://www.justice.gov/usao-sdny/pr/us-attorney-announces-historic-336-billion-cryptocurrency-seizure-and-conviction

[52] *See:* https://www.justice.gov/opa/pr/two-arrested-alleged-conspiracy-launder-45-billion-stolen-cryptocurrency

Thus, if a sophisticated cryptocurrency actor transferred illicitly acquired assets to a privately held wallet and the government hasn't acquired the private keys, there isn't an avenue for seizure. Unless the funds need to be immediately liquidated, this makes cryptocurrency an excellent vehicle for stashing away illicitly acquired funds. That being said, OFAC can still sanction the wallet address(s), severely limiting the means through which an actor could convert that cryptocurrency to fiat.

While the USG has made big strides, the number of investigators and prosecutors versed in how to identify and seize illicit cryptocurrency assets is still low compared to the number of investigators and prosecutors well versed in fiat asset tracing and seizure.

C. Government Officials May Nonetheless Convert Gains Into Cryptocurrency as an Investment Tactic, Using Similar Strategies to Obscure True Ownership

The cryptocurrency industry is no longer operating in the "Wild West" as it was in its infancy. The majority of VASPs have robust AML/KYC programs and powerful blockchain analysis tools with robust attribution data. More importantly, the USG has shown that it has crypto-savvy investigators and the means to affect large cryptocurrency seizures. The belief that cryptocurrency offers financial anonymity for illicit actors has largely been debunked at this point. However, as the cryptocurrency industry has matured, illicit actors have developed a heightened sense of operational security and use newer financial products like DeFi and DEXs in sophisticated money laundering typologies.

If a crypto savvy actor effectively used a combination of VASPs or P2P/OTC exchanges that do not collect KYC information, privately held wallets, privacy coins, DeFi platforms like DEXs, and cryptocurrency mixers, it would be next to impossible to for the USG to track and seize those funds. Illicit actors can also leverage "money laundering for hire" groups on the dark web or purchase, for a sizable fee, cryptocurrency stolen via other illicit activity to obfuscate the source of their funds. The price volatility of cryptocurrencies, and common use as a speculative investment vehicle, could also be used to the advantage of an actor seeking to obfuscate the true ownership of funds. Once an actor has taken steps to obfuscate the source of funds (in fiat or cryptocurrency), they can be converted to one or multiple cryptocurrencies and cashed out when their original value has substantially increased.

This takes an extraordinary amount of effort, but is certainly doable for a motivated actor, and state sponsored actors like the Russian, Chinese, and DPRK Advanced Persistent Threat (APT) groups have repeatedly shown that they have the desire and talent to do so. Under the right set of circumstances, government officials seeking to circumvent ABC and AML measures could use cryptocurrency to great effect to obscure the true ownership and destination of illicitly acquired funds.