International
Comparative
Legal Guides

Practical cross-border insights into sanctions

Sanctions 2022

Third Edition

Contributing Editors:
Roberto J. Gonzalez & Rachel M. Fiorill
Paul, Weiss, Rifkind, Wharton & Garrison LLP

ICLG.com

Expert Analysis Chapters

Q&A Chapters

No End in Sight: An Update on the Rising Risk and Recent Developments in Cryptocurrency Sanctions and Enforcement

Guidehouse

Adam Klauder

I Introduction

Countries around the globe continue to use economic sanctions as a targeted means of implementing foreign policy objectives. By their nature, sanctions evolve continuously to address new threats and to advance a particular government's current foreign policy objectives. Due to its seamless peer-to-peer transfer capabilities, pseudo-anonymous qualities, and the still-maturing regulatory environment in which it exists, cryptocurrency has become an attractive alternative for criminals and other malign actors that seek to evade sanctions and move illicit funds across international borders.[1] Governments and regulators are responding to this rising risk through new guidance, regulation, and enforcement. Since the initial publication of this chapter in the 2020 edition of the *ICLG – Sanctions* guide, the pace of these developments has been swift and shows no sign of slowing down. This chapter will provide an updated overview of recent cryptocurrency developments for 2021, particularly as they relate to economic sanctions.

II Cryptocurrency Background

Cryptocurrencies are digital representations of value that, unlike government-issued fiat currency, do not have any status as legal tender. Some digital assets are "centralised", meaning they have a central payment ledger that is run by a centralised administrator who issues currency. Cryptocurrencies, on the other hand, use "distributed" ledger technology (e.g., blockchain), to enable individual computers within peer-to-peer networks to record and share transactions in their respective electronic ledgers. Bitcoin, Ether, and Litecoin are some of the most well-known types of cryptocurrencies and are designed to function as a medium of exchange or payment for goods and services.[2]

Most cryptocurrencies use cryptographic protocols to both secure the ledger and make sure transactions that are recorded on the blockchain are public. Cryptocurrencies provide "pseudo-anonymity" to users because although a transaction can be associated with a specific cryptocurrency address, the name of the actual address holder is not visible on the blockchain and can remain anonymous.[3] Law enforcement and the commercial sector have developed forensic and monitoring tools to help identify illicit actors who are associated with particular cryptocurrency addresses, but technology that allows individuals to process financial transactions with any level of anonymity can create a significant risk that sanctions evaders could seek to exploit.

Virtual currency exchanges provide platforms for customers to either trade cryptocurrencies for other cryptocurrencies, or to trade cryptocurrencies for fiat currency. Similar to banks, many virtual currency exchanges also store cryptocurrency for their customers. Most jurisdictions regulate cryptocurrency exchanges as financial institutions, usually as money transmitters or payment services. Deemed to be money transmitters, virtual currency exchanges in the United States are required to comply with the Bank Secrecy Act (BSA) and its associated regulations, which involves conducting due diligence on customers and maintaining adequate anti-money laundering (AML) controls.[4] In addition, the U.S., along with other countries and governmental bodies, have well-developed economic sanctions programmes that apply to cryptocurrency exchanges regardless of their regulatory status.

III U.S. Economic Sanctions and Cryptocurrency Developments

A. U.S. Economic Sanctions Overview

Economic sanctions are a tool that governments use to achieve foreign policy objectives by targeting specific individuals, entities, governments, and/or countries. In the United States, the Department of the Treasury's Office of Foreign Assets Control (OFAC) implements and administers economic sanctions under applicable U.S. laws.[5] Generally, U.S. economic sanctions seek to deprive targets of the use of their assets and/or to deny them the benefits of trade and commerce with the United States.

All "U.S. persons" must comply with U.S. economic sanctions. This includes any U.S. citizen, permanent resident alien, entity organised under the laws of the United States, or any person in the United States. In the case of some OFAC sanctions, the prohibitions also apply to non-U.S. entities that are owned or controlled by U.S. persons.

U.S. economic sanctions can take the form of primary sanctions, which include list-based blocking sanctions that prohibit U.S. persons from undertaking almost all transactions related to the individuals and entities found on the list of Specially Designated Nationals and Blocked Persons (SDN). In addition, country-based embargoes prohibit U.S. persons from undertaking almost all transactions with a listed jurisdiction. Finally, list-based sectoral sanctions prohibit U.S. persons from undertaking limited, specific transactions with listed entities. Secondary sanctions seek to deter non-U.S. persons from engaging in a range of activities even if they do not involve any U.S. elements.

B. OFAC Cryptocurrency Developments

In March 2018, OFAC took an initial public step to address how it will treat compliance obligations relating to cryptocurrency by publishing five frequently asked questions (FAQs).[6] These

FAQs confirm that a U.S. person's OFAC compliance obligations remain the same, regardless of whether a transaction is denominated in digital currency or in traditional fiat currency, and recommend that U.S. technology companies, payment processors, and digital currency administrators, exchangers, and users "develop a tailored, risk-based compliance program, which generally should include sanctions-list screening and other appropriate measures".[7] OFAC further signalled that it might include digital currency addresses associated with blocked persons as identifiers on the SDN List.[8] OFAC explained that parties who hold cryptocurrency and identify digital currency identifiers or wallets that they believe are owned by, or otherwise associated with, an SDN should take the necessary steps to block the relevant digital currency and file a report with OFAC that includes information about the wallet's or address's ownership, and any other relevant details.[9] Importantly, OFAC clarified that "persons that provide financial, material, or technological support for or to a designated person may be designated by OFAC under the relevant sanctions authority".[10] By publishing these FAQs, OFAC put the financial community on notice as to the level of compliance it expects from those who are engaged in cryptocurrency transactions.

In November 2018, OFAC added two additional FAQs, which addressed technical requirements relating to blocking digital currency.[11] Most notably, however, was OFAC's designation in the same action of two Iran-based individuals as SDNs for their involvement in financial transactions related to the "SamSam" ransomware scheme.[12] In the scheme, the illicit cyber actors required victims to pay a "ransom" in bitcoin to regain access to and control of their data. The two SDNs were digital currency exchangers who helped the cyber actors exchange the bitcoin into Iranian rial and deposit it into Iranian banks. In the SDN listing for these two individuals, OFAC for the first time listed digital currency addresses in the identifying information. OFAC highlighted the significance of this action in its press release, and stated that "[l]ike traditional identifiers, these digital currency addresses should assist those in the compliance and digital currency communities in identifying transactions and funds that must be blocked and investigating any connections to these addresses".[13] OFAC coordinated its designations with related law enforcement actions against two other Iranian criminal actors by the Department of Justice (DOJ) and the FBI.[14]

OFAC published digital currency addresses as identifiers again in August 2019 when it designated three individuals, one company, and the Zheng Drug Trafficking Organization (DTO) as significant foreign narcotics trafficker SDNs under the Foreign Narcotics Kingpin Designation Act.[15] The press release referenced a related indictment that was also unsealed, which noted that the Zheng DTO "laundered its drug proceeds in part by using digital currency such as bitcoin, transmitted drug proceeds into and out of bank accounts in China and Hong Kong, and bypassed currency restrictions and reporting requirements".[16] Almost a year later, OFAC designated four additional individuals as SDNs for providing support to the Zheng DTO, and one company for being owned or controlled by the Zheng DTO.[17]

In October 2020, OFAC and the Financial Crimes Enforcement Network (FinCEN) issued concurrent advisories on the sanctions and AML risks relating to ransomware and the facilitation of ransomware payments (FinCEN's advisory will be discussed in Section IV.A. below). OFAC's advisory addresses the increase in ransomware payments demands over the past few years and the risks of making such payments, including that they will be made to parties with a sanctioned nexus and/or used to harm the national security interests of the United States.[18] OFAC states clearly that any ransomware payments made to sanctioned parties could result in penalties that are subject to strict liability and that any licence applications involving ransomware payments will be reviewed by OFAC on a case-by-case basis with a presumption of denial. OFAC's advisory does, however, outline the steps that companies should take if they are victims of a ransomware attack, and notes that it would "consider a company's self-initiated, timely, and complete report of a ransomware attack to law enforcement to be a significant mitigating factor in determining an appropriate enforcement outcome if the situation is later determined to have a sanctions nexus".[19]

In September 2021, OFAC issued an updated ransomware advisory, which builds on the previous guidance by highlighting additional ways companies can mitigate these types of sanctions risks proactively.[20] This includes improving or adopting robust cybersecurity practices, such as those that are highlighted in the Cybersecurity and Infrastructure Security Agency's September 2020 Ransomware Guide.[21] OFAC strongly encourages companies to cooperate with law enforcement and other relevant U.S. agencies during and after a ransomware attack, which, along with other mitigating steps, it would view as a "significant mitigating factor" during any potential enforcement action and would be more likely to resolve through a non-public response such as a No Action Letter or a Cautionary Letter.[22]

OFAC has continued to add digital currency addresses to the SDN List, including in April 2021, when it published a list of cryptocurrency addresses tied to alleged Russian governmental interference in U.S. elections.[23] These addresses were associated with a wide range of digital assets, including Bitcoin, Bitcoin Cash, Litecoin, Zcash, Dash, Verge and Ether.

In May 2021, OFAC updated FAQ 594, which had stated previously that it was not possible to search for digital currency addresses against OFAC's Sanctions List Search tool. The updated FAQ now reflects that such searches are possible, though only exact matches will be recognised (i.e., there is no "fuzzy logic").[24]

Finally, in September 2021, OFAC added a virtual currency exchange (SUEX OTC, S.R.O.) to the SDN List for the first time due to its role in facilitating ransomware-related financial transactions.[25]

C. State-sponsored Virtual Currencies

Many countries, including the United States, United Kingdom, and China, have explored creating state-sponsored or central bank cryptocurrencies. These efforts, which could create a means of transferring currency outside the traditional banking system, could pose a significant challenge to countering the sanctions evasion ambitions of countries such as Iran, North Korea, Russia and Venezuela.

1. Iran

In July 2018, Iran announced that it intended to launch a national cryptocurrency, which would be pegged to the rial, its national fiat currency.[26] News reports indicated that the Iranian government has subsequently sought to ban any unapproved cryptocurrencies for payment purposes, but that it would permit individuals to hold small amounts of non-governmental cryptocurrencies for personal (i.e., non-commercial) purposes.[27] Regardless of the obvious tension that exists in Iran between the regime's development of a centralised national cryptocurrency and the desire of Iranian citizens to utilise decentralised cryptocurrencies, Iranians in both the government and the private sector will likely continue to look for ways to use this new type of asset to mitigate the ongoing economic effects of international sanctions.

2. Venezuela

In December 2017, Venezuela announced its plans to launch a state-sponsored cryptocurrency backed by oil reserves and

commodities (the petro).[28] In response, President Trump issued Executive Order 13827[29] and OFAC issued additional FAQs that prohibit U.S. persons from engaging in transactions involving petros.[30] In March 2019, OFAC also designated Evrofinance Mosnarbank, a Moscow-based bank that is jointly owned by Russian and Venezuelan state-owned companies, as an SDN. OFAC described the bank as "the primary international financial institution willing to finance the petro".[31]

Although the petro has struggled to gain widespread traction as a viable currency alternative, Venezuela has developed a growing peer-to-peer market for cryptocurrency to protect against rising inflation.[32] In a recent action that could further impact Venezuela's petro ambitions, the United States has placed Joselit de la Trinidad Ramirez Camacho, the superintendent of Venezuela's petro initiative, on its "Most Wanted List" due to his alleged involvement in narcotics trafficking.[33]

In August 2021, Venezuela announced that it would launch the country's first central bank digital currency, which will coincide with a "monetary redenomination" to address high levels of inflation.[34] The Central Bank of Venezuela is expected to begin circulating the new digital Venezuelan bolivar in October 2021.

3. North Korea

News reports indicate that North Korea is also developing its own official cryptocurrency in a likely attempt to circumvent sanctions, though it appears to only be in the early stages of creation at the moment.[35] With respect to cryptocurrency, North Korea is more well known for its state-sponsored cyber campaigns to hack cryptocurrency exchanges and launch ransomware attacks, as well at its cryptocurrency mining efforts. For example, the North Korean-linked Lazarus Group has been implicated in the 2017 WannaCry ransomware attack, which affected hundreds of thousands of computers worldwide, including the United Kingdom's National Health Service.[36] In September 2018, the United States filed charges against Lazarus Group member Park Jin Hyok for his involvement in this ransomware attack, along with his involvement in "the 2016 theft of $81 million from Bangladesh Bank; the 2014 attack on Sony Pictures Entertainment; and numerous other attacks or intrusions on the entertainment, financial services, defense, technology, and virtual currency industries, academia, and electric utilities".[37] In 2021, the DOJ unsealed an indictment against Park Jin Hyok and two other North Korean computer programmers for these wide-ranging offences.[38] The indictment also detailed a scheme to develop and market a digital token (the "Marine Chain Token"), which would allow investors to purchase fractional ownership interests in marine shipping vessels. According to the indictment, the purpose of this scheme was to evade U.S. sanctions, and the involvement of North Korean individuals was not disclosed during the perpetrators' attempts to obtain funds from investors.

4. Russia

Although Russia has shown some resistance to fully embracing the use of cryptocurrencies, it has begun exploring the development of a state-sponsored cryptocurrency, with Russian officials stating that the primary goal is to "settle accounts with our counterparties all over the world with no regard for sanctions".[39] In addition, news reports indicate that the Russian government was instrumental in helping Venezuela develop its state-sponsored petro cryptocurrency.[40] There had been a fear within Russia that all cryptocurrency activity would be banned as Russia and its central bank continue to work through how to maintain control over the cryptocurrency market without allowing its prevalence to erode the domestic markets and currency. Recently, however, Russia enacted a new cryptocurrency law that, beginning in 2021, will permit Russians to mine, own, and trade cryptocurrencies on exchanges as long as the cryptocurrency is not used for domestic goods and services.[41] Similar to Venezuela, Russia is making progress on developing a central bank digital currency, with a prototype slated to be ready by the end of 2021.[42]

IV Sanctions and Regulatory Landscape

In addition to OFAC, other U.S. and global agencies such as FinCEN, the Financial Action Task Force (FATF), the DOJ, and the UN have been involved in developing guidance to raise awareness around the use of cryptocurrency for illicit purposes.

A. FinCEN

FinCEN implements, administers, and enforces compliance with the BSA and its associated regulations. In March 2013, FinCEN clarified that administrators and exchangers of virtual currency are considered money services business (MSB) money transmitters and must register as such with FinCEN, as well as implement relevant AML recordkeeping, reporting, and compliance measures.[43] Since that time, FinCEN has been active in issuing guidance relating to cryptocurrencies and in helping financial institutions identify and address cryptocurrency compliance issues.

In October 2018, FinCEN issued an advisory on the Iranian regime's attempts to exploit the international financial system.[44] This advisory sought to help U.S. financial institutions (including virtual currency administrators and exchangers) better detect potentially illicit transactions involving Iran. The advisory cautioned that although cryptocurrency is not used widely in Iran, it is "an emerging payment system that may provide potential avenues for individuals and entities to evade sanctions". As such, FinCEN urged financial institutions to consider reviewing blockchain ledgers for activity that may originate or terminate in Iran and advised them to be aware of person-to-person exchangers (i.e., natural or legal persons who offer to buy, sell, or exchange virtual currency through online sites and in-person meetups) that may offer services in Iran. The advisory reminded financial institutions that a non-U.S.-based exchanger or virtual currency provider doing substantial business in the United States is subject to AML/Combating the Financing of Terrorism (CFT) obligations, as well as OFAC jurisdiction.

In May 2019, FinCEN issued an additional advisory on illicit activity such as money laundering and sanctions evasion involving "convertible virtual currencies" (CVCs).[45] Specifically, the advisory highlights prominent typologies such as darknet marketplaces, peer-to-peer exchangers, foreign-located MSBs, and CVC kiosks, along with associated red flags. FinCEN issued concurrent guidance on how its regulations apply to certain businesses that transact in CVCs, which consolidated FinCEN's previously issued guidance on this subject.[46] FinCEN reiterated its general position that any person engaging in the business of money transmission or the transfer of funds, including CVCs, must (1) maintain an effective written AML programme, and (2) register as an MSB. FinCEN also required money transmitters that engage in a "transmittal of funds" to comply with the "Funds Transfer Rule"[47] and "Funds Travel Rule".[48]

During a speech in December 2019, FinCEN Director Ken Blanco noted that shortly after FinCEN issued its May advisory on illicit activity involving CVCs there were over 2,100 unique suspicious activity report (SAR) filers that referenced the key terms from the advisory, many of whom had not filed SARs previously.[49] With respect to cryptocurrencies, Director Blanco stated, "I think it is important for all financial institutions to ask

themselves whether they are reporting such suspicious activity. If the answer is no, they need to reevaluate whether their institutions are exposed to cryptocurrency".[50]

As mentioned previously, FinCEN and OFAC released advisories in October 2020 to address the financial crime risks associated with ransomware and facilitating ransomware payments. The FinCEN advisory focuses on the role of financial intermediaries in the processing of ransomware payments, and outlines some of the current trends and typologies of ransomware and associated payments.[51] Some trends and typologies include cybercriminals targeting of larger enterprises to demand bigger payouts (i.e., "big game hunting") and the use of anonymity-enhanced cryptocurrencies in illegal activity. The FinCEN advisory also lists 10 financial red flag indicators of ransomware-related illicit activity and reminds financial institutions of their reporting and information-sharing obligations related to ransomware attacks. In particular, FinCEN directs financial institutions to reference "CYBER-FIN-2020-A006" and include a narrative description in their SARs when there is a connection between the suspicious activity being reported and ransomware-related activity.

B. FATF

On June 21, 2019, FATF released new guidance governing virtual assets and virtual asset service providers.[52] The new FATF standards require all countries to regulate and supervise such service providers, including exchangers, and to mitigate against such risks when engaging in cryptocurrency transactions. This guidance represents a significant step toward strengthening international compliance standards around cryptocurrencies and recommends that the sector comply with the same AML/CFT requirements as traditional financial institutions. In June 2020, FATF issued a report that summarised its 12-month review of the industry's progress in implementing the new standards.[53] The report noted that 35 out of 54 reporting jurisdictions have implemented the revised FATF Standards and did not identify a clear need to amend the standards. It also acknowledged the progress that countries have made in implementing the "travel rule", which requires virtual asset service providers to obtain, hold and exchange information about the originators and beneficiaries of virtual asset transfers.[54] FATF issued its second 12-month review report in July 2021, which noted that even though an increased number of countries have implemented the revised FATF Standards and taken enforcement action against rule violators, most jurisdictions still have not implemented comprehensive AML/CFT requirements for virtual assets.[55] In addition, the report noted that most jurisdictions are still not in compliance with the travel rule.

C. DOJ

On October 8, 2020, the DOJ Office of the Deputy Attorney General's Cyber-Digital Task Force, published "Cryptocurrency: An Enforcement Framework" (the Framework), which highlights the emerging criminal and national security threat that cryptocurrency use poses to the U.S. and provides detailed information about the DOJ's approach to combatting the illicit uses of cryptocurrency and related technologies.[56] The Framework begins with an overview of cryptocurrency and some of its key characteristics (e.g., decentralised in nature, varying degrees of anonymity), and then describes in some detail both the legitimate and illegitimate uses of this type of virtual asset. In focusing on the ways in which malicious actors leverage cryptocurrency for criminal and illegal purposes, the Framework identifies various ways in which cryptocurrency can be used for illicit activity, including to commit crimes, support terrorism, or to hide financial activity. The Framework provides examples of recent enforcement actions that highlight various criminal schemes involving cryptocurrency, such as cases relating to ransomware, darknet markets, terrorist financing, money laundering, and operating unlicensed money services businesses. It also presents the current cryptocurrency regulatory landscape, including applicable laws and regulations, as well as relevant regulatory authorities. In its final section, the Framework identifies the types of business models and activities that may facilitate cryptocurrency-related criminal activity, as well as strategies that DOJ expects to deploy in response.

D. United Nations

The UN has published two recent annual reports that detail the extent to which North Korea has violated international sanctions, from procuring weapons of mass destruction to evading sanctions through maritime transactions. These reports also detail some of the disruptive strategies that North Korea has been using to increase its financial position through both the theft and use of cryptocurrencies.

The August 2019 UN Panel of Experts Report listed 35 potential instances in which persons and/or entities affiliated with North Korea have attempted to generate revenue by engaging in cyber-related attacks on financial institutions, and stealing/mining cryptocurrency.[57] The report notes that a large number of targets in South Korea have come under attack by North Korea-affiliated entities, including the Bithub and Youbit cryptocurrency exchanges. In addition, the report describes how North Korea-affiliated actors have used cryptocurrency to launder bitcoin that was paid by victims of the WannaCry ransomware attacks.

The United Nations published a follow-up report in March 2020, where it highlighted additional ways in which North Korea has sought to generate illicit cryptocurrency revenue in contravention of international sanctions.[58] One unique way was by hosting a cryptocurrency conference in Pyongyang, which sought to involve experts from around the world. Virgil Griffith, a U.S. person who attended the 2019 conference, has been charged with violating U.S. sanctions. According to the pleadings, conference organisers instructed Griffith to explain how to use cryptocurrency and blockchain technology to evade sanctions and launder money.[59] In advance of the proposed February 2020 conference in North Korea there were press reports about the UN's warnings that attendance could constitute sanctions evasion.[60]

The March 2020 UN Panel of Experts Report also details an additional cyber-attack by North Korea-affiliated actors against a cryptocurrency exchange that utilised a "Trojan horse" malware application, which allowed the hackers to control their victims' computer systems and access and steal cryptocurrency.[61]

V Recent Enforcement Actions

March 2020 – DOJ Criminal Action Against Two Chinese Nationals for Laundering Over $100 Million in Cryptocurrency from Exchange Hack

On March 2, 2020, the U.S. Department of Justice charged Chinese nationals Jiadong Li and Yinyin Tian with laundering over $100 million worth of cryptocurrency from a hack of a cryptocurrency exchange.[62] In a coordinated action, OFAC designated Li and Tian as SDNs and added 20 new bitcoin addresses associated with these two individuals to the SDN List.[63] The

civil forfeiture complaint specifically names 113 virtual currency accounts and addresses that were used by the defendants and unnamed co-conspirators to launder funds.

According to the pleadings, Li and Tian stole approximately $250 million in cryptocurrency by hacking into a virtual currency exchange. To launder the funds, Li and Tian circumvented the compliance controls at various virtual currency exchanges by submitting falsified "know your customer" information and used "peel chains" to launder the stolen cryptocurrency and obscure the source of funds. In a peel chain, criminals "peel" off a small amount of cryptocurrency from a larger amount during a transaction. The process is repeated until all of the cryptocurrency has been sent to new addresses and it is often deposited into various virtual currency exchanges. Li and Tian spent several months using peel chains to transfer and convert much of the stolen cryptocurrency into regular currency at Chinese banks. The pleadings also indicate that Li and Tian sold some of the stolen cryptocurrency to U.S. customers and routed some of the funds through a U.S.-based cryptocurrency exchange.

On August 27, 2020, DOJ filed a civil forfeiture complaint to seize 280 cryptocurrency accounts containing funds that were laundered by the same group of Chinese actors.[64] This action also represents the first publicly announced case where North Korean hackers have targeted a U.S. virtual currency exchange.[65]

August 2020 – DOJ's "Global Disruption of Three Terror Finance Cyber-Enabled Campaigns"

On August 13, 2020, DOJ announced that it had dismantled three cyber-related terrorist financing campaigns involving the al-Qassam Brigades (Hamas's military wing), al-Qaeda, and Islamic State of Iraq and the Levant (ISIS).[66] DOJ noted that this coordinated operation was the U.S. government's largest-ever seizure of cryptocurrency in the terrorism context, involving millions of dollars and over 300 cryptocurrency accounts.

According to the pleadings, the al-Qassam Brigades, which along with Hamas is designated by OFAC as an SDN, sought to solicit bitcoin donations to fund terrorism. U.S. law enforcement worked covertly to monitor and operate al-Qassam Brigade websites, which led to the seizure of approximately 150 cryptocurrency accounts that contained these illicit donations. The al-Qaeda campaign also involved solicitation for bitcoin donations to fund terrorism and used layering techniques to launder and obscure the source of the funds. U.S. law enforcement is seeking the forfeiture of the 155 virtual currency assets tied to this terrorist campaign. Finally, in the separate ISIS campaign, an ISIS hacker set up a website (FaceMaskCenter.com) and four Facebook pages to sell N95 respirator masks that had not been approved by the U.S. Food and Drug Administration. DOJ officials noted separately that the complaints did not identify any financial crime control failures at the institutions and regulated exchanges that handled the illicit cryptocurrency at issue.[67]

December 2020 – OFAC Enters Into $98,830 Settlement with BitGo, Inc., for Apparent Violations of Multiple Sanctions Programs Related to Digital Currency Transactions

On December 30, 2020, OFAC announced its first enforcement action against a digital assets company. In the enforcement release, OFAC alleged that between approximately March 2015 and December 2019, California-based BitGo, Inc. (BitGo) had processed 183 digital currency transactions on behalf of individuals located in Crimea, Cuba, Iran, Sudan, and Syria, using BitGo's "hot wallet" secure digital management service. According to OFAC, BitGo collected and tracked its users' Internet Protocol (IP) addresses for security purposes related to account logins but did not use this same IP address information to identify and mitigate sanctions compliance risk. OFAC also noted that although BitGo amended its practices to require all new accountholders to verify the country in which they were located beginning in April 2018, the company relied on user attestations and did not conduct additional verification or diligence on the location of its account holders.

This enforcement action is significant not only because it is the first one brought publicly by OFAC, but also because of the examples OFAC provides for good compliance practices for digital assets companies in the "mitigating factors" section of the enforcement release. OFAC notes that BitGo had invested in significant remedial measures, including hiring a chief compliance officer and implementing a new OFAC policy. With respect to BitGo's policy, OFAC highlighted the following items, including:

- A detailed overview of OFAC and relevant sanctions laws.
- The appointment of a compliance officer specifically responsible for implementing and providing guidance and interpretation on matters related to U.S. sanctions laws.
- IP address blocking, as well as email-related restrictions, for sanctioned jurisdictions.
- Periodic batch screening.
- Record-keeping procedures for all financial records and documentation related to sanctions compliance efforts.
- A review and, where appropriate, update of end-user agreements to ensure that customers are aware of, and comply with, U.S. sanctions requirements.
- A review of screening configuration criteria on a periodic basis.

Even though OFAC determined that BitGo did not voluntarily disclose the matter and could have been subject to a maximum civil monetary penalty of approximately $53 million, it determined that the case was "non-egregious" and entered into a settlement for $98,830.

February 2021 – OFAC Enters Into $507,375 Settlement with BitPay, Inc., for Apparent Violations of Multiple Sanctions Programs Related to Digital Currency Transactions

Shortly after the BitGo enforcement action was released, OFAC announced its second enforcement action against a digital assets company. On February 18, 2021, OFAC issued an enforcement release in which it is alleged that BitPay, Inc. (BitPay) had processed 2,102 transactions between approximately June 2013 and September 2018 on behalf of individuals who were located in Crimea, Cuba, North Korea, Iran, Sudan, and Syria. BitPay is an Atlanta-based company that provides a payment processing solution for merchants to accept payment for goods in digital currency. OFAC alleged that although BitGo conducted sanctions screening on the merchants, who were BitGo's direct customers, it did not screen the information it had in its possession relating to the merchants' buyers, including their names, addresses, email addresses, and phone numbers.

Even though OFAC determined that BitPay did not voluntarily disclose the matter and could have been subject to a maximum civil monetary penalty of approximately $620 million, it determined that the case was "non-egregious" and entered into a settlement for $507,375.

VI Looking Toward the Future

There have been a number of important "firsts" and enforcement developments in the past year that highlight sanctions compliance issues and address potential sanctions evasion concerns, from OFAC bringing its first enforcement action against a digital assets company to the recent guilty plea from the former chief of darknet-based cryptocurrency "mixing" service Helix to money laundering conspiracy charges.[68] Even with increased guidance and law enforcement focus, however, illicit actors will likely continue attempting to exploit gaps in the regulatory framework and the ease of peer-to-peer transfer to use cryptocurrency to avoid economic sanctions. As a result, those who have cryptocurrency compliance obligations should review their compliance programmes to ensure that they are comprehensive and take current developments into account.

Consistent with OFAC's compliance guidance, firms should conduct a risk assessment to identify potential OFAC issues that might exist as the result of their involvement with cryptocurrencies. In addition, institutions should update their screening capabilities to incorporate the latest blockchain analytics solutions or engage with a vendor that can provide these services. Finally, firms should provide training to employees on blockchain technology, sanctions evasion typologies that are unique to cryptocurrencies, and recent developments in the cryptocurrency regulatory and enforcement area.

Endnotes

1. This chapter uses the term "cryptocurrency" to refer generally to "digital currency", "virtual currency", "virtual assets" and other similar terms to describe digital representations of value that can be traded digitally and function like money.
2. Rebecca M. Nelson, "Examining Regulatory Frameworks for Digital Currencies and Blockchain", Testimony before the U.S. Senate Committee on Banking, Housing, and Urban Affairs, July 30, 2019, https://crsreports.congress.gov/product/pdf/TE/TE10034.
3. Toshendra Kumar Sharma, "How is Blockchain Verifiable by Public and Yet Anonymous?", Blockchain Council, July 10, 2018, https://www.blockchain-council.org/blockchain/how-is-blockchain-verifiable-by-public-and-yet-anonymous/.
4. 31 U.S.C. § 5311 *et seq.*
5. In addition to OFAC, other U.S. governmental agencies help enforce sanctions, including: (i) Department of State; (ii) Department of Justice; and (iii) the Department of Commerce, Bureau of Industry and Security (BIS). Many non-U.S. countries and governmental organisations also administer sanctions internationally, including: (i) the United Nations (UN); (ii) the European Union (EU); and (iii) the United Kingdom (Office of Financial Sanctions Implementation).
6. OFAC FAQs, Questions on Virtual Currency, https://home.treasury.gov/policy-issues/financial-sanctions/faqs/topic/1626.
7. *Id.*
8. OFAC FAQ 561, https://home.treasury.gov/policy-issues/financial-sanctions/faqs/topic/1626.
9. OFAC FAQ 562, https://home.treasury.gov/policy-issues/financial-sanctions/faqs/topic/1626.
10. OFAC FAQ 560, https://home.treasury.gov/policy-issues/financial-sanctions/faqs/topic/1626.
11. OFAC FAQs 646 and 647, https://home.treasury.gov/policy-issues/financial-sanctions/faqs/topic/1546.
12. OFAC, "Cyber-related Designations; Publication of New Cyber-related FAQs", November 18, 2018, https://home.treasury.gov/policy-issues/financial-sanctions/recent-actions/20181128.
13. 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.
14. U.S. Department of Justice, Press Release: "Two Iranian Men Indicted for Deploying Ransomware to Extort Hospitals, Municipalities, and Public Institutions, Causing Over $30 Million in Losses", November 28, 2018, https://www.justice.gov/opa/pr/two-iranian-men-indicted-deploying-ransomware-extort-hospitals-municipalities-and-public.
15. OFAC, "Kingpin Act Designations", August 21, 2019, https://home.treasury.gov/policy-issues/financial-sanctions/recent-actions/201 90821.
16. U.S. Department of the Treasury, Press Release: "Treasury Targets Chinese Drug Kingpins Fueling America's Deadly Opioid Crisis", August 21, 2019, https://home.treasury.gov/news/press-releases/sm756.
17. U.S. Department of the Treasury, Press Release: "Treasury Targets Chinese Persons Involved with Drug Trafficking Organization Moving Fentanyl", July 17, 2020, https://home.treasury.gov/news/press-releases/sm1063; OFAC, "Counter Narcotics Designations; Counter Narcotics Designations Removals and Update; Nicaragua-related Designations", July 17, 2020, https://home.treasury.gov/policy-issues/financial-sanctions/rece nt-actions/20200717.
18. OFAC, "Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments," October 1, 2020, https://home.treasury.gov/system/files/126/ofac_ransomware_advisory_10012020_1.pdf.
19. *Id.*
20. OFAC, "Updated Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments", September 21, 2021, https://home.treasury.gov/system/files/126/ofac_ransomware_advisory.pdf.
21. *Id.*; *see also* Cybersecurity and Infrastructure Security Agency Guidance, *Ransomware Guide*, September 2020, https://www.cisa.gov/sites/default/files/publications/CISA_MS-ISAC_Ransomware%20Guide_S508C_.pdf.
22. OFAC, "Updated Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments", September 21, 2021, https://home.treasury.gov/system/files/126/ofac_ransomware_advisory.pdf.
23. OFAC, "Issuance of Executive Order Blocking Property With Respect To Specified Harmful Foreign Activities Of The Government Of The Russian Federation and related Frequently Asked Questions; Russia-related Designations", April 15, 2021, https://home.treasury.gov/policy-issues/financial-sanctions/recent-actions/20210415.
24. OFAC FAQ 594, https://home.treasury.gov/policy-issues/financial-sanctions/faqs/topic/1626.
25. OFAC, "Publication of Updated Ransomware Advisory; Cyber-related Designation", https://home.treasury.gov/policy-issues/financial-sanctions/recent-actions/20210921.
26. Tanvi Ratna, "Iran Has a Bitcoin Strategy to Beat Trump", Foreign Policy, January 24, 2020, https://foreignpolicy.com/2020/01/24/iran-bitcoin-strategy-cryptocurrency-blockchain-sanctions/.
27. Leigh Cuen, Stan Higgins, "Iran Could Ban Bitcoin for Payments, Central Bank Report Suggests", coindesk, January 29, 2019, https://www.coindesk.com/iran-could-ban-bitcoin-for-payments-central-bank-report-suggests.

28. "Venezuela Plans a Cryptocurrency, Maduro Says", *The New York Times*, December 3, 2017, https://www.nytimes.com/2017/12/03/world/americas/venezuela-cryptocurrency-maduro.html.
29. Executive Order 13827, "Taking Additional Steps to Address the Situation in Venezuela", 83 Fed. Reg. 55, March 21, 2018, https://home.treasury.gov/system/files/126/13827.pdf.
30. OFAC, "Issuance of Venezuela-related Executive Order; Venezuela-related Designations; Publication of new Venezuela-related Frequently Asked Questions; Publication of new Digital Currency-related Frequently Asked Questions", March 19, 2018, https://home.treasury.gov/policy-issues/financial-sanctions/recent-actions/2018 0319.
31. 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.
32. Caitlin Reilly, "Venezuelans use cryptocurrency to bypass corruption, inflation", Roll Call, September 10, 2019, https://www.rollcall.com/2019/09/10/venezuelans-use-cryptocurrency-to-bypass-corruption-inflation/.
33. Paddy Baker, "US Offers $5M Bounty for Arrest of Venezuela's Crypto Chief", coindesk, June 2, 2020, https://www.coindesk.com/us-venezuela-petro-most-wanted.
34. Cointelegraph, "Venezuela to launch CBDC in October – And cut six zeros from its currency", August 6, 2021, https://cointelegraph.com/news/venezuela-to-launch-cbdc-in-october-and-cut-six-zeros-from-its-currency.
35. David Gilbert, "North Korea Is Building Its Own Bitcoin", Vice News, September 18, 2019, https://www.vice.com/en_us/article/9ke3ae/north-korea-is-building-its-own-bitcoin.
36. Chris Graham, "NHS Cyber Attack: Everything You Need to Know About the 'Biggest Ransomware' Offensive in History", The Telegraph, May 20, 2017, https://www.telegraph.co.uk/news/2017/05/13/nhs-cyber-attack-everything-need-know-biggest-ransomware-offensive/.
37. U.S. Department of Justice, "North Korean Regime-Backed Programmer Charged With Conspiracy to Conduct Multiple Cyber Attacks and Intrusions", September 6, 2018, https://www.justice.gov/opa/pr/north-korean-regime-backed-programmer-charged-conspiracy-conduct-multiple-cyber-attacks-and.
38. U.S. Department of Justice, "Three North Korean Military Hackers Indicted in Wide-Ranging Scheme to Commit Cyberattacks and Financial Crimes Across the Globe," February 17, 2021, https://www.justice.gov/opa/pr/three-north-korean-military-hackers-indicted-wide-ranging-scheme-commit-cyberattacks-and.
39. Max Seddon and Martin Arnold, "Putin considers 'cryptorouble' as Moscow seeks to evade sanctions", Financial Times, January 1, 2018, https://www.ft.com/content/54d026d8-e4cc-11e7-97e2-916d4fbac0da.
40. Simon Shuster, "Exclusive: Russia Secretly Helped Venezuela Launch a Cryptocurrency to Evade U.S. Sanctions", TIME, March 20, 2018, https://time.com/5206835/exclusive-russia-petro-venezuela-cryptocur rency/.
41. Roger Huang, "Russia Backs Away From Total Cryptocurrency Ban", Forbes, August 10, 2020, https://www.forbes.com/sites/rogerhuang/2020/08/10/russia-backs-away-from-total-cryptocurrency-ban/#2a095c707520.
42. CNBC, "Digital currencies are the future for Russia's financial system, central bank governor says," June 2, 2021, https://www.cnbc.com/2021/06/02/digital-currencies-are-the-future-for-russia-central-bank-chief-says.html.
43. FinCEN Guidance, FIN-2013-G001, "Application of FinCEN's Regulations to Person's Administering, Exchanging, or Using Virtual Currencies", March 18, 2013, https://www.fincen.gov/sites/default/files/shared/FIN-2013-G001.pdf.
44. 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://fas.org/irp/world/iran/fincen-102018.pdf.
45. FinCEN Advisory, FIN-2019-A003, "Advisory on Illicit Activity Involving Convertible Virtual Currency", May 9, 2019, https://www.fincen.gov/sites/default/files/advisory/2019-05-10/FinCEN%20Advisory%20CVC%20FINAL%20508.pdf.
46. FinCEN Guidance, FIN-2019-G001, "Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies", May 9, 2019, https://www.fincen.gov/sites/default/files/2019-05/FinCEN%20Guidance%20CVC%20FINAL%20508.pdf.
47. 31 CFR § 1010.410(e).
48. 31 CFR § 1010.410(f).
49. Ken Blanco, American Bankers Association/American Bar Association, Financial Crimes Enforcement Conference, December 10, 2019, https://www.fincen.gov/news/speeches/prepared-remarks-fincen-director-kenneth-blanco-delivered-american-bankers.
50. *Id.*
51. FinCEN Advisory, FIN-2020-A006, "Advisory on Ransomware and the Use of the Financial System to Facilitate Ransom Payments", October 1, 2020, https://www.fincen.gov/sites/default/files/advisory/2020-10-01/Advisory%20Ransomware%20FINAL%20508.pdf.
52. FATF, "Guidance for a Risk-Based Approach, Virtual Assets and Virtual Service Providers", June 21, 2019, https://www.fatf-gafi.org/media/fatf/documents/recommendations/RBA-VA-VASPs.pdf.
53. FATF, "12-month Review of the Revised FATF Standards on Virtual Assets and Virtual Asset Service Providers", June 2020, https://www.fatf-gafi.org/media/fatf/documents/recommendations/12-Month-Review-Revised-FATF-Standards-Virtual-Assets-VASPS.pdf.
54. Although progress has been made in this area, compliance will remain difficult to achieve until a workable technology solution is developed.
55. FATF, "Second 12-month Review of the Revised FATF Standards on Virtual Assets and Virtual Asset Service Providers", July 2021, https://www.fatf-gafi.org/media/fatf/documents/recommendations/Second-12-Month-Review-Revised-FATF-Standards-Virtual-Assets-VASPS.pdf.
56. DOJ, "Report of the Attorney General's Cyberdigital Task Force: Cryptocurrency Enforcement Framework", October 2020, https://www.justice.gov/archives/ag/page/file/1326061/download.
57. United Nations, "Report of the Panel of Experts established pursuant to resolution 1874 (2009)", August 30, 2019, http://undocs.org/S/2019/691.
58. United Nations, "Report of the Panel of Experts established pursuant to resolution 1874 (2009)", March 2, 2020, https://undocs.org/S/2020/151.
59. Southern District of New York, *United States of America v. Virgil Griffith*, Case No. 19MAG10987, Complaint, November 21, 2019, https://www.justice.gov/usao-sdny/press-release/file/1222646/download.
60. Michele Nichols, "Exclusive: U.N. sanctions experts warn — stay away from North Korea cryptocurrency conference", Reuters, January 15, 2020, https://www.reuters.

com/article/us-northkorea-sanctions-un-exclusive/exclusive-u-n-sanctions-experts-warn-stay-away-from-north-korea-cryptocurrency-conference-idUSKBN1ZE0I5.
61. United Nations, "Report of the Panel of Experts established pursuant to resolution 1874 (2009)", March 2, 2020, https://undocs.org/S/2020/151.
62. U.S. Department of Justice Press Release, "Two Chinese Nationals Charged with Laundering Over $100 Million in Cryptocurrency from Exchange Hack", March 2, 2020, https://www.justice.gov/opa/pr/two-chinese-nationals-charged-laundering-over-100-million-cryptocurrency-exchange-hack.
63. U.S. Department of the Treasury Press Release, "Treasury Sanctions Individuals Laundering Cryptocurrency for Lazarus Group", March 2, 2020, https://home.treasury.gov/news/press-releases/sm924.
64. U.S. Department of Justice Press Release, "United States Files Complaint to Forfeit 280 Cryptocurrency Accounts Tied to Hacks of Two Exchanges by North Korean Actors", August 27, 2020, https://www.justice.gov/opa/pr/united-states-files-complaint-forfeit-280-cryptocurrency-accounts-tied-hacks-two-exchanges.
65. Ian Talley, "U.S. Moves to Seize Cryptocurrency Accounts Linked to North Korean Heists", *Wall Street Journal*, August 27, 2020, https://www.wsj.com/articles/u-s-moves-to-seize-cryptocurrency-accounts-linked-to-north-korean-heists-11598564571.
66. U.S. Department of Justice Press Release, "Global Disruption of Three Terror Finance Cyber-Enabled Campaigns", August 13, 2020, https://www.justice.gov/opa/pr/global-disruption-three-terror-finance-cyber-enabled-campaigns.
67. Valentina Pasquali, "US Prosecutors Announce 'Historic' Takedown of Global Terrorists' Crypto Networks", ACAMS moneylaundering.com, August 13, 2020, https://www.moneylaundering.com/news/us-prosecutors-announce-historic-takedown-of-global-terrorists-crypto-networks/?source=Keyword%20Alert%20-%20Daily&utm_campaign=&utm_medium=email&utm_source=Eloqua&utm_source_code=.
68. DOJ, "Ohio Resident Pleads Guilty to Operating Darknet-Based Bitcoin 'Mixer' That Laundered Over $300 Million", August 18, 2021, https://www.justice.gov/opa/pr/ohio-resident-pleads-guilty-operating-darknet-based-bitcoin-mixer-laundered-over-300-million.

Adam Klauder is a senior director in Guidehouse's Global Investigations and Compliance practice. He is a seasoned compliance executive, attorney, and senior leader with an extensive background in developing overall compliance strategy, directing and coordinating sensitive and high-profile global investigations, and providing strategic guidance on the build-out of corporate compliance functions. Mr. Klauder advises clients in the defence, healthcare, financial services, transportation and logistics, energy and infrastructure, and telecommunications sectors, and is a subject matter expert in compliance matters involving economic sanctions, export controls, anti-corruption, cryptocurrency, and other cross-border regulatory regimes. Prior to joining Guidehouse, Mr. Klauder was a senior global compliance executive at HSBC, serving as Global Head of Sanctions Investigations and Global Investigations Advisor.

Guidehouse
1200 19th Street, NW
Suite 700
Washington, D.C. 20036
USA

Tel: +1 202 481 8371
Email: adam.klauder@guidehouse.com
URL: www.guidehouse.com

ICLG.com

Current titles in the ICLG series

Alternative Investment Funds
Anti-Money Laundering
Aviation Finance & Leasing
Aviation Law
Business Crime
Cartels & Leniency
Class & Group Actions
Competition Litigation
Construction & Engineering Law
Consumer Protection
Copyright
Corporate Governance
Corporate Immigration
Corporate Investigations
Corporate Tax
Cybersecurity
Data Protection
Derivatives
Designs
Digital Business
Digital Health
Drug & Medical Device Litigation
Employment & Labour Law
Enforcement of Foreign Judgments
Environment & Climate Change Law
Environmental, Social & Governance Law
Family Law
Fintech
Foreign Direct Investment Regimes
Franchise
Gambling
Insurance & Reinsurance
International Arbitration
Investor-State Arbitration
Lending & Secured Finance
Litigation & Dispute Resolution
Merger Control
Mergers & Acquisitions
Mining Law
Oil & Gas Regulation
Patents
Pharmaceutical Advertising
Private Client
Private Equity
Product Liability
Project Finance
Public Investment Funds
Public Procurement
Real Estate
Renewable Energy
Restructuring & Insolvency
Sanctions
Securitisation
Shipping Law
Technology Sourcing
Telecoms, Media & Internet
Trade Marks
Vertical Agreements and Dominant Firms

The International Comparative Legal Guides are published by: glg global legal group