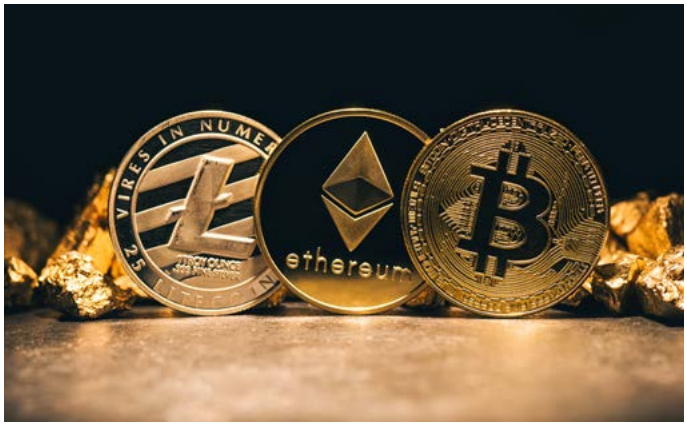
Cryptocurrency and sanctions evasion: meeting the challenge

There's little conclusive evidence that cryptocurrencies are being used to evade sanctions. But any concerns are justified, with some lawmakers calling out OFAC's enforcement procedures as lacking requisite muscle. Here, Sam Amir Toossi sets out the arguments – and makes recommendations to industry to limit its own related risks.

In the aftermath of Russia's invasion of Ukraine, the US and its Western allies swiftly imposed sweeping sanctions on Russia designed to cripple its economy. Shortly thereafter, a wave of media articles described the effort of some Russian actors to use cryptocurrency to evade the sanctions. While the extent to which cryptocurrency has been or is being used to circumvent the sanctions regime is currently unknown, its reputation for enabling transactions outside of the traditional financial ecosystem has heightened concerns that it could potentially be exploited for sanctions evasion.

Although the blockchain technology that underpins cryptocurrency means transactions can be traced through the general ledger, it can be difficult but not impossible for the relevant government entities to trace and link the illegal transactions back to real persons. And because cryptocurrency transactions occur outside traditional financial systems and institutions, which have mature compliance programmes, regulators are correct to be concerned that cryptocurrency and digital assets might be used to circumvent US sanctions.

US policymakers in all branches of government have shared this concern. Recently, Senator Elizabeth Warren (D-MA) wrote a letter to Treasury Secretary Janet Yellen inquiring about the Treasury Department's progress enforcing and monitoring sanctions compliance by the cryptocurrency industry. In the same letter, Senator Warren expressed her concern that the Treasury Department's Office of Foreign Assets Control ('OFAC') 'has not developed sufficiently strong and effective procedures for enforcement in the cryptocurrency industry'.



Senator Warren is not alone among her Senate colleagues on this issue. On 17 March 2022, the Senate Banking Committee held a hearing on the potential use of cryptocurrencies to evade US sanctions. Although experts from the cryptocurrency community discounted concerns that such evasion could happen at scale – citing transparent, permanent records in blockchain technology – the senators on the committee were clearly sceptical.

The Senate's concern is clearly shared by the Biden administration. On 9 March 2022, President Biden signed Executive Order 14067 on Ensuring Responsible Development of Digital Assets, specifically listing 'sanctions evasion' among the issues presented by digital assets such as cryptocurrencies.

These issues are not entirely new, as federal regulators have been grappling for the past few years with the impact of cryptocurrency and other digital assets on sanctions enforcement. The recent sanctions on Russia merely heighten the focus on the issue. This article discusses the efforts that federal regulators in the Department of Justice ('DoJ') and the Treasury Department have taken to enforce sanctions compliance in the cryptocurrency industry, as well as a recent judicial opinion released on the issue. In addition, it recommends some steps that companies can take to protect themselves from inadvertently violating the sanctions when transacting in cryptocurrency and other digital assets.

Current enforcement framework

Understanding the underlying enforcement framework is key when considering OFAC and the DoJ's recent enforcement activities and their implications for the users of cryptocurrency and sanctions compliance. OFAC may impose civil penalties based on a strict liability legal standard,[1] meaning, liability does not depend on negligence or intent to violate, and OFAC only has the burden to prove that the apparent violation occurred. Where there is evidence that a violation was made willfully, OFAC may impose civil penalties and refer the matter to other law enforcement agencies like the DoJ for criminal investigation and/or prosecution.[2] The DoJ bears responsibility for pursuing criminal violations, namely those violations that are committed willfully and knowingly in violation of US sanctions.

When determining the appropriate enforcement response, OFAC takes into consideration the totality of facts and circumstances surrounding the apparent violation. Each factor might be considered mitigating or aggravating, resulting in a lower or higher proposed penalty amount.[3] Pursuant to 31 C.F.R. Part 501, OFAC can impose

civil monetary penalties for sanctions violations which are currently capped at $330,947 (subject to annual adjustment for inflation)[4] or twice the amount of the transaction found to have violated the law, whichever is higher. However, if a US person voluntarily self-discloses any apparent violation to OFAC, the amount of the proposed civil penalty may be reduced to 50%.[5] Companies are encouraged to adopt risk-based compliance programmes recommended by OFAC, which can also be mitigating factors in reducing the civil monetary penalties.

OFAC's actions in the cryptocurrency space

OFAC has taken the position that sanctions compliance obligations apply equally to transactions involving cryptocurrency and traditional currency.[6] While the sanctions imposed on Russia in response to its invasion of Ukraine have put a spotlight on the use of cryptocurrency to evade US sanctions, OFAC's guidance and recent enforcement history demonstrate an increasingly focused effort toward enforcing sanctions compliance in the cryptocurrency space.

These efforts include sanctioning individuals and entities that have used cryptocurrency in connection with unlawful activities. For example, in March 2020, OFAC sanctioned two Chinese nationals involved in laundering stolen cryptocurrency by Lazarus Group, a North Korean state-sponsored organisation. In 2018, Lazarus Group conducted a cyber-attack to steal $250 million worth of virtual currencies from a cryptocurrency exchange. Two Chinese nationals received approximately $100 million and layered the funds in transactions to convert $1.4 million worth of Bitcoin into prepaid iTunes gift cards.[7] More recently, on 23 March 2022, Lazarus Group carried out the largest virtual currency heist in history – worth almost $620 million – from a blockchain project linked to an online game. Lazarus Group used virtual currency mixer Blender.io to process over $20.5 million of the illicit proceeds.[8] OFAC subsequently issued its first-ever sanctions on a virtual currency mixer, Blender.io., signalling OFAC's commitment to exposing components of the virtual currency ecosystem that are part of the illicit cyber activity.

Although OFAC has published only two enforcement actions regarding cryptocurrency, each reflects how the agency analyses relevant factors to calculate a final civil monetary penalty. On 30 December 2020, OFAC entered into a settlement with BitGo, Inc., a technology company based in California that offers non-custodial secure digital wallet management services, for apparent violations of multiple sanctions programmes related to digital currency transactions. In the published settlement, OFAC stated that, since 2015, BitGo processed 183 cryptocurrency transactions, totaling $9,127.79, on behalf of individuals located in sanctioned jurisdictions. Due to the number of transactions, OFAC determined that the statutory maximum civil monetary penalty was $53,051,675. However, OFAC deemed the violations to be 'non-egregious', and despite the fact that BitGo did not voluntarily self-disclose the violations, the agency determined that the base civil monetary penalty was $183,000. The settlement amount of $93,830 reflected OFAC's considerations of the totality of circumstances, including aggravating factors – BitGo's failure to prevent persons apparently located in sanctioned jurisdictions to open accounts, its failure to implement appropriate risk-based sanctions compliance controls and that it had reasons to know the location of these users based on IP addresses associated with the login devices – and certain mitigating factors, such as the company's implementation of remedial measures (including the retroactive screening of all users) and its cooperation with the agency's investigation.

THOUGH CRYPTOCURRENCIES ARE STILL IN THE NASCENT PHASE OF REGULATION THE US GOVERNMENT IS QUICKLY CENTERING ON A COHESIVE APPROACH.

Soon thereafter, on 18 February 2021, OFAC announced its second settlement of an enforcement action related to cryptocurrency – a $507,375 settlement with BitPay, Inc., a technology company based in the state of Georgia. BitPay offers a payment processing platform for merchants to accept cryptocurrency as payment for goods and services. According to the settlement, although BitPay had location information, including IP addresses, about customers in sanctioned jurisdictions, the company failed to prevent them from using its platform to engage in $129,000 worth of cryptocurrency transactions. Even though BitPay has implemented sanctions compliance controls since 2013, the deficiencies in the company's compliance programme allowed the violation to occur, which OFAC deemed an aggravating factor. However, OFAC also considered remedial measures taken by BitPay (including terminating conduct that led to the apparent violations and cooperating with OFAC's investigations) and reduced the base civil monetary penalty from $2,255,000 to $507,375.[9]

There are several key takeaways from OFAC enforcement actions in and its guidance to the cryptocurrency sector. The first is, unsurprisingly, that OFAC will strongly credit self-reporting of violations, raising the onus on companies to review their cryptocurrency transactions and giving them the incentive to assist OFAC in identifying violations. Second, OFAC has signaled that it will treat cryptocurrency platforms through the same lens that it views traditional financial institutions, heightening the emphasis on compliance programmes designed to prevent violations in the first place.

The practical effect is that cryptocurrency platforms – many still in a considerably nascent phase – are not equal. Indeed, users of cryptocurrencies should evaluate the platform's compliance programmes and determine whether they are sufficient to prevent an inadvertent sanctions violation.

DoJ establishes KleptoCapture, signaling DoJ enforcement to come

The DoJ's recent activity clearly demonstrates that it intends to pursue criminal charges against wilful sanctions violators. On 2 March 2022, the DoJ established the interagency Task Force KleptoCapture, an interagency effort to enforce the sanctions and export restrictions against Russia in response to its invasion of Ukraine.[10] As news reports abounded of Russian efforts to evade the sanctions using cryptocurrency, the DoJ stated that part of the KleptoCapture's mission would be to 'target… efforts to use cryptocurrency to evade US sanctions, launder proceeds of foreign corruption, or evade US responses to Russian military aggression.' OFAC also issued guidance in a frequently asked question released on 11 March 2022, confirming that compliance with the Russian sanctions would be required 'regardless of whether a transaction is denominated in traditional fiat currency or virtual currency.'

The DoJ's announcement of the task force not only signaled that many US and international institutions having Russian clients will be facing significant scrutiny in sanctions compliance, but also signaled criminal penalties against using cryptocurrency to evade sanctions will come. On 12 April 2022, the US Attorney's office in the Southern District of New York announced an indictment against a US citizen, Virgil Griffith – who allegedly conspired to provide advice to North Korea on using cryptocurrency and blockchain technology to evade sanctions. Griffith was sentenced to over five years in prison and fined $100,000. According to court

documents, Griffith presented at the 'Pyongyang Blockchain and Cryptocurrency Conference' and provided instruction on how to use cryptocurrency to launder money and evade sanctions.

According to the DoJ allegations, Griffith also developed and funded technology infrastructures to mine cryptocurrency in North Korea. After the conference, Griffith facilitated the exchange of cryptocurrency between North Korea and South Korea, despite knowing that these transactions violated sanctions against North Korea.[11] The DoJ subsequently traced the illicit transactions to two European citizens, who were then charged for conspiring with Griffith to assist North Korea's sanction evading. As alleged, two European individuals, Alejandro Cao De Benos and Christopher Emms, provided blockchain and cryptocurrency services to North Korea while advising the regime on how to use these technologies to evade sanctions.[12]

US REGULATORS VIEW SANCTIONS COMPLIANCE AS TRANSACTION BASED, MEANING THAT THE FORM OF PAYMENT IS IMMATERIAL AND THE ONUS IS ON THE USERS OF CRYPTOCURRENCY TO ENSURE COMPLIANCE WITH EXISTING SANCTIONS.

The US judiciary weighs in

As discussed above, the US executive branch clearly intends to clamp down on sanctions evaders using cryptocurrency. Now, the US District Court for the District of Columbia ('DDC') has weighed in, confirming that the DoJ can pursue criminal charges against individuals that use cryptocurrency to evade US sanctions. This ruling not only confirms that the DoJ is pursuing sanctions violators criminally, but it also represents the first time that the federal courts have approved of such enforcement.

On 13 May, US Magistrate Judge Zia Faruqui, sitting in the DDC, ruled that the DoJ could pursue a criminal action based on the use of cryptocurrency to evade US sanctions. In an opinion rich with pop-culture references (including *Friday the 13th*, *Silicon Valley* and *Saturday Night Live*), the Court stated that '[T]he question is no longer whether virtual currency is here to stay… but instead whether fiat currency regulations will keep pace with frictionless and transparent payments on the blockchain.'[13] The Court ultimately relied heavily on OFAC's recent guidance from October 2021, which determined that 'Sanctions compliance obligations apply equally to transactions involving virtual currencies and those involving traditional fiat currencies.'[14] Notably, the Court also cited with approval OFAC's settlement of enforcement actions with BitGo and BitPay, giving the judiciary's approval to the logic of those settlements.

There are several key takeaways from Judge Faruqui's opinion. First, while it is unknown which sanctioned country was involved in the transactions at issue, the DoJ has been clear that it intends to pursue sanctions violators criminally. As Deputy Attorney General Lisa Monaco recently said, 'Sanctions are the new FCPA.'[15] And the opinion reveals that the DoJ is now pursuing sanctions violations using cryptocurrency criminally. Second, it is unusual that the opinion is even available to the public. The case remains under seal, and the Court redacted the name of the defendant and the sanctioned country at issue. And yet the Court nonetheless published the opinion on its website, seemingly as a warning that not only does the executive branch (e.g., DoJ and OFAC) view cryptocurrency as subject to sanctions regulations, but the judiciary does now as well. Indeed, there is now clear judicial precedent for the proposition that the use of cryptocurrency is subject to US sanctions. As Judge Faruqui stated in his opinion, 'The [DoJ] can and will criminally prosecute individuals and entities for failure to comply with [sanctions] regulations, including as to virtual currency.'

How should market actors respond?

The key takeaway is that regulators view sanctions compliance as transaction based, meaning that the form of payment is immaterial and the onus is on the users of cryptocurrency to ensure compliance with existing sanctions. Although cryptocurrencies are still in the nascent phase of regulation, what is clear is that the US government is quickly centering on a cohesive strategy and approach.

To this end, as the popularity and use of cryptocurrency proliferated, in October 2021, OFAC issued Sanctions Compliance Guidance for the Virtual Currency Industry to outline a framework for companies to mitigate the risk of sanction violations. The guidance notes that a tailored and risk-based compliance programme will vary depending on the company's size and sophistication, products and services, customers, and geolocations. However, in its guidance, OFAC advised that companies should adopt and incorporate at least five essential sanction compliance components recommended by the guidance, specifically: (1) management commitment, (2) risk assessment, (3) internal controls, (4) testing and auditing, and (5) training.[16] OFAC's two enforcement actions in this space indicate that companies incorporated at least some of these five components will reduce the risk of exposure to violation and mitigate penalties if the apparent violation is found.

An effective compliance programme will include know-your-customer procedures, transaction monitoring, and geolocation tools to identify and prevent IP addresses that originate in sanctioned jurisdictions.[17] Remedial measures are also mitigating factors to reduce penalties.[18] Therefore, even upon learning apparent violations have occurred, companies should lean heavily towards self-reporting and take steps to enhance compliance. These two mitigation steps can work in tandem because some actions intended to mitigate risk could be viewed as assisting clients in evading sanctions. For example, terminating a client relationship could remove the assets from the DoJ's jurisdiction. Therefore, self-reporting before remedial steps are taken is critical to staying in compliance with US regulations.

Sam Amir Toossi is a partner in Akrivis Law Group's New York office and heads the firm's White Collar Defense and Commercial Litigation practice. Mr Toossi would like to thank his law clerk, Xander Peng, for his assistance in writing this article.

HTTPS://AKRIVISLAW.COM

LINKS AND NOTES

[1] See e.g., *Sanctions Compliance Guidance for the Virtual Currency Industry, Office of Foreign Assets Control* (October 2021), https://home.treasury.gov/system/files/126/virtual_currency_guidance_brochure.pdf.
[2] See 31 C.F.R. Part 501.
[3] Id.
[4] See *Inflation Adjustment of Civil Monetary Penalties*, Federal Register (Feb. 9, 2022) https://www.federalregister.gov/documents/2022/02/09/2022-02736/inflation-adjustment-of-civil-monetary-penalties.
[5] See supra note 1, at 9,
[6] See e.g., *Sanctions Compliance Guidance for the Virtual Currency Industry, Office of Foreign Assets Control* (October 2021), https://home.treasury.gov/system/files/126/virtual_currency_guidance_brochure.pdf.
[7] See Press Release, U.S. Dep't of the Treasury, Treasury Sanctions Individuals Laundering Cryptocurrency for Lazarus Group (Mar. 2, 2020), https://home.treasury.gov/news/press-releases/sm924.
[8] See Press Release, U.S. Dep't of the Treasury, U.S. Treasury Issues First-Ever Sanctions on a Virtual Currency Mixer, Targets DPRK Cyber Threats (May 6, 2022), https://home.treasury.gov/news/press-releases/jy0768.
[9] See Press Release, U.S. Dep't of the Treasury, OFAC Enters Into $507,375 Settlement with BitPay, Inc. for Apparent Violations of Multiple Sanctions Programs Related to Digital Currency Transactions (Feb. 18, 2021), https://home.treasury.gov/system/files/126/20210218_bp.pdf.
[10] See U.S. Dep't of Justice, 'Attorney General Merrick B. Garland Announces Launch of Task Force KleptoCapture' (Mar. 2, 2022), https://www.justice.gov/opa/pr/attorney-general-merrick-b-garland-announces-launch-task-force-kleptocapture.
[11] See Press Release, U.S. Dep't of Justice, *U.S. Citizen Who Conspired to Assist North Korea in Evading Sanctions Sentenced to Over Five Years and Fined $100,000* (Apr. 12, 2022), https://www.justice.gov/opa/pr/us-citizen-who-conspired-assist-north-korea-evading-sanctions-sentenced-over-five-years-and.
[12] See Press Release, U.S. Dep't of the Justice, *Two European Citizens Charged for Conspiring with a U.S. Citizen to Assist North Korea in Evading U.S. Sanctions* (Apr. 25, 2022), https://www.justice.gov/opa/pr/two-european-citizens-charged-conspiring-us-citizen-assist-north-korea-evading-us-sanctions.
[13] *In Re: Criminal Complaint*, No. 22-mj-067-ZMF, at 4 (D.D.C. May. 13. 2022)
[14] *Id*. (quoting OFAC, Sanctions Compliance Guidance for Virtual Currency ('OFAC Guidance'), at 1 (Oct. 2021), https://home.treasury.gov/system/files/126/virtual_currency_guidance_brochure.pdf; see also U.S. Dep't of the Treasury, Questions on Virtual Currency (Mar. 19, 2018), https://home.treasury.gov/policy-issues/financial-sanctions/faqs/560.
[15] Dylan Tokar, *Sanctions Turn Into New Priority for Justice Department*, The Wall Street Journal, https://libguides.uakron.edu/c.php?g=627783&p=6800463 (last visited Jun. 17, 2022)
[16] See *supra* note 1, at 11-19.
[17] See *supra* note 1, at 13-15.
[18] See *supra* note 1, at 16.

Reprinted with permission from the July-August 2022 issue of *WorldECR*, the journal of export controls and sanctions.

www.worldecr.com