NORTON ROSE FULBRIGHT

Blockchain Law

Cryptocurrency offers no escape from international sanctions

By Robert A. Schwinger, *New York Law Journal* — March 9, 2021

Recent US enforcement activity illustrates how the government is taking strong action against persons involved with misuses of cryptocurrency in order to meet this threat and deter others.

Among the conclusions offered in the "Cryptocurrency Enforcement Framework" issued by the Department of Justice this past fall (see generally R. Schwinger, "Blockchain Law: DOJ's 'Cryptocurrency Enforcement Framework," NYLJ (Jan. 15, 2021)) was the ominous warning that "cryptocurrency presents a troubling new opportunity for individuals and rogue states to avoid international sanctions and to undermine traditional financial markets, thereby harming the interests of the United States and its allies." A spate of recent government enforcement action shows that the United States is not hesitating to tackle cryptocurrency activity being used to try to circumvent the prohibitions of US economic sanctions.

The United States maintains a powerful system of economic sanctions as part of the tools it uses in international relations, such as under the International Emergency Economic Powers Act, 50 U.S.C. §§1701 et seq. (IEEPA). These sanctions target not just particular bad actors but also certain entire countries or regimes. Well-known examples of such sanctioned states include North Korea, Iran, Cuba, Venezuela, Crimea, Sudan and Syria. These sanctions are designed to cut off these countries from much of the modern financial system, as a means of U.S. leverage in international relations.

For persons in or involved with such sanctioned countries, the prospect of being able to make and receive payments through cryptocurrency outside the conventional financial system with its stringent regulations and oversight is a powerful lure, especially given the ability cryptocurrency offers to operate anonymously or pseudonymously. But recent U.S. enforcement activity illustrates how the government is taking strong action against persons involved with such misuses of cryptocurrency in order to meet this threat and deter others.

Talk, services or conspiracy?

In *United States v. Griffith*, 2020 WL 275903 (S.D.N.Y. Jan. 27, 2021), the Court upheld an indictment charging a U.S. citizen with conspiring to violate IEEPA sanctions against North Korea by giving a talk in Pyongyang on blockchain technology and cryptocurrency. The defendant Griffith was an employee of the Ethereum Foundation, which supports the Ethereum blockchain. His indictment centered on a presentation he made at a cryptocurrency conference in North Korea concerning possible applications of blockchain technology.

It was charged that prior to this conference, Griffith had been interested in establishing an Ethereum environment in North

Robert A. Schwinger is a partner in the commercial litigation group at Norton Rose Fulbright US LLP.

Korea, at one point texting a colleague that "we'd love to make an Ethereum trip to [North Korea] and setup an Ethereum node … . It'll help them circumvent the current sanctions on them." He also sent texts to a colleague speculating that while he was not sure why North Korea was interested in cryptocurrencies, it was "probably avoiding sanctions." Despite the State Department's denial of a request Griffith made for permission to travel to North Korea to speak at the cryptocurrency conference about "the applications of blockchain technology to business and anti-corruption," Griffith nevertheless was able to secure a visa from North Korea's mission to the UN in New York and spoke at the conference.

The court held that Griffith's presentation constituted the prohibited export of a service to North Korea, a country subject to comprehensive U.S. sanctions. See Exec. Order 13722, 81 Fed. Reg. 14943 (March 15, 2016); 31 C.F.R. §510.206(a). In so holding, the court rejected several defenses Griffith had raised.

Griffith argued that his presentation could not constitute services because he was not paid, but the court rejected the contention that the receipt of a fee is a necessary element of a "service." It pointed to *United States v. Banki*, 685 F.3d 99 (2d Cir. 2012), which rejected any fee requirement, relying on the dictionary definition of "service" as well as the policy consideration that if services required a fee to be prohibited, parties would be at liberty to provide uncompensated assistance to persons subject to sanctions without any consequences.

Griffith also raised the issue that U.S. sanctions on North Korea, like other U.S. sanctions programs, exempt "informational materials" from the prohibition on the export of services, and argued that his conduct fell within the exemption. The regulation from the Treasury Department's Office of Foreign Asset Control (OFAC) on which Griffith relied, however, limited this exemption to materials "fully created and in existence at the date of the transactions." 31 C.F.R. §510.213(c)(2). The court thus rejected Griffith's attempt to challenge his indictment on this ground. It stated that "the key distinction rests between informational materials that are widely circulated in a standardized format and those that are bespoke" (quoting *United States v. Amirnazmi*, 645 F.3d 564, 587 (3d Cir. 2011)). While Griffith argued that his presentation was nothing more than "high-level publicly available information" without substantive alteration, and consisted of only "general articles in the public domain" and "very general information … available on the Internet," the government claimed to have evidence that Griffith drew diagrams on a whiteboard while speaking and concluded his time with a brief question-and-answer session. The court concluded that whether Griffith's presentation was fully created and in existence at the date of the presentation was a factual dispute that a jury would have to resolve.

The court also held that ultimately these issues did not affect the validity of the indictment because Griffith was charged with conspiracy to violate IEEPA, not a substantive IEEPA violation. The government charged that Griffith and his co-conspirators agreed to advise North Korea on how "to evade and avoid sanctions by using blockchain and cryptocurrency technologies" and that "Griffith's speaking engagement at the April 2019 conference was a major step in a long-term plan to persuade and assist [North Korea] in using Ethereum to avoid sanctions and launder money." The indictment alleged that the presentation was simply one action in furtherance of a conspiracy that extended from August 2018 through November 2019 (seven months after the speaking engagement). The act in furtherance of the conspiracy did not itself need to be illegal.

Lastly, the court rejected Griffith's contention that the indictment as applied to him violated his First Amendment right to free speech. It concluded that even under a strict scrutiny approach the IEEPA regulatory scheme as applied to Griffith did not violate the First Amendment because it served a compelling foreign policy interest of the United States—maintaining national security—while imposing the least restrictive burden on speech. It determined that the regulatory scheme was narrowly tailored to meet this compelling interest because it was aimed at a designated country, exempted information or informational materials from its coverage, implemented a licensing scheme that permits U.S. persons to apply for authorization to provide services, and required the government to prove willful misconduct beyond a reasonable doubt.

The court stressed that Griffith's challenge to his indictment "has nothing to do with advocacy" but rather with knowingly and willfully participating in a conspiracy to provide services to North Korea. In addition, it noted, "[s]ervices by their nature are intangible and are often rendered through the

words of the service-provider, whether lawyer, accountant, financial advisor or technology advisor." Thus, as an "alternative holding," the court concluded that because speech concerning cryptocurrency transactions or blockchain technology is "an essential but subordinate component" of the service in question, "it lowers the level of appropriate judicial scrutiny." The challenge to the indictment thus withstood the defendant's attack on First Amendment grounds as well, notwithstanding that the crime charged centered around giving a talk at a conference.

Cryptocurrency in the North Korean military intelligence toolkit

On Feb. 17, 2021, the Justice Department unsealed a two-count indictment that had been returned on Dec. 8, 2020 against three North Korean officials. These officials, alleged to be part of a North Korean military intelligence agency called the Reconnaissance General Bureau, were charged with various illicit cyber, cryptocurrency and blockchain activities, including as part of an attempt to evade U.S. sanctions. *United States v. Jon Chang Hyok, Kim Il and Park Jin Hyok*, No 2:20-cr-00614-DMG (C.D. Cal.). In the first count, the indictment charged the defendants with conspiracy under 18 U.S.C. §371 to violate various provisions of the Computer Fraud and Abuse Act, 18 U.S.C. §1030, by orchestrating various cyber intrusions and attacks, heists and ransomware attacks, and by spreading malware, against victims that included entertainment companies, financial institutions, online casinos, and cryptocurrency companies. The indictment's second count charged the defendants with conspiracy in violation of 18 U.S.C. §1349 to commit bank and wire fraud through various schemes, one of which involved using a cryptocurrency initial coin offering (ICO) and blockchain tokenization of assets for purposes that included evading U.S. sanctions.

Specifically, the indictment's second count alleged that defendant Kim Il and other conspirators developed a plan to create a digital token called the "Marine Chain Token," which would allow investors to "purchase fractional ownership interests in marine shipping vessels, such as cargo ships, supported by a blockchain." Defendant Kim Il would contact individuals in Singapore, where he once lived, regarding potential involvement in creating Marine Chain. He and the other conspirators were also alleged at times to have used false and fraudulent names when contacting individuals they hoped would be involved in creating Marine Chain, not disclosing that they were North Korean citizens or that they were communicating using false and fraudulent names.

The indictment further charged that as part of the defendants' plan, they sought to raise funds for the Marine Chain platform through an ICO. In doing so, they allegedly communicated with potential investors using false and fraudulent names in order to convince them to invest in the Marine Chain platform, again not disclosing they were North Korean citizens or that they were communicating using false and fraudulent names. The indictment also charged that they would not disclose to investors that "a purpose of the Marine Chain Token was to evade United States sanctions on North Korea." According to the allegations, their plan was to "tokenize individual vessels on the Marine Chain platform, allowing investors to purchase ownership interests in marine shipping vessels," and to receive approval from Hong Kong's Securities and Futures Commission to trade the Marine Chain Token as a security.

According to a New York Times report, a Justice Department official acknowledged that there was little chance that any of the three defendants, who live in North Korea, would be arrested. Nevertheless, the official explained that the indictment was intended to show the public the seriousness of the North Korean threat and the Justice Department's ability to identify persons involved in such activities and to warn them and the countries that support them.

More than just North Korea

Concern about cryptocurrency being used as a means to evade IEEPA sanctions is not limited to North Korea. Three years ago, President Trump issued Executive Order 13827 (March 19, 2018) directed against Venezuela, in response to Venezuela's efforts to bypass the effect of U.S. economic sanctions by developing its own cryptocurrency called the "Petro."

This Executive Order states that:

> in light of recent actions taken by the Maduro regime to attempt to circumvent U.S. sanctions by issuing a digital currency in a process that Venezuela's democratically elected National Assembly has denounced as unlawful … [a]ll transactions related to, provision of financing for, and other dealings in, by a United States person or

> within the United States, any digital currency, digital coin, or digital token, that was issued by, for, or on behalf of the Government of Venezuela on or after January 9, 2018, are prohibited … .

The order further prohibits "[a]ny transaction that evades or avoids, has the purpose of evading or avoiding, causes a violation of, or attempts to violate any of the prohibitions set forth in th[e] order" and "[a]ny conspiracy formed to violate any of the prohibitions set forth in this order."

The order specifically provides that its references to the "Government of Venezuela" are intended to encompass "any political subdivision, agency, or instrumentality" of that governments, "including the Central Bank of Venezuela and Petroleos de Venezuela, S.A. (PdVSA)" as well as any other person or entity "owned or controlled by, or acting for or on behalf of, the Government of Venezuela."

Due diligence risks for domestic companies

On February 18, 2021, OFAC issued an Enforcement Release in which it announced that an Atlanta-based company called BitPay, Inc., which offered a payment processing solution to enable merchants to accept digital currency as payment for goods and services, had agreed to pay $507,375 to settle potential civil liability for what OFAC charged were "2,102 apparent violations of multiple sanctions programs." The OFAC release charged that BitPay

> allowed persons who appear to have been located in the Crimea region of Ukraine, Cuba, North Korea, Iran, Sudan, and Syria to transact with merchants in the United States and elsewhere using digital currency on [its] platform even though [it] had location information, including Internet Protocol (IP) addresses and other location data, about those persons prior to effecting the transactions.

OFAC explained in its release that "[w]hile BitPay screened its direct customers—the merchants" against OFAC sanctions lists, it allegedly "failed to screen location data that it obtained about its merchants' buyers," which reportedly included the buyers' names, addresses, email addresses, phone numbers and IP addresses. As a result, even though BitPay had implemented certain sanctions compliance controls and made clear in employee training that it prohibited merchant sign-ups from sanctioned jurisdictions and trade with sanctioned individuals and entities, OFAC sought and was able to obtain civil penalties against BitPay.

OFAC stressed:

> This action highlights that companies involved in providing digital currency services … should understand the sanctions risks associated with providing digital currency services and should take steps necessary to mitigate those risks. Companies that … process transactions using digital currency are responsible for ensuring that they do not engage in unauthorized transactions prohibited by OFAC sanctions, such as dealings with blocked persons or property, or engaging in prohibited trade or investment-related transactions.

Conclusion

Cryptocurrencies and other virtual and digital currencies seek to stake their place in the financial world alongside more conventional financial products and instruments and better known and more historically familiar banks and financial institutions. But in so doing, it should come as little surprise that this new asset class will likewise find itself falling subject to tools like the economic sanctions the United States uses to protect its international interests by wielding power over global financial markets and international transactions. For the United States not to do so would expose it to the risk that its sanctions regime could be rendered toothless by new financial technology. Players in the cryptocurrency space who ignore the restrictions imposed by U.S. international sanctions are being put on notice that they do so at their peril.