Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

US Actions Show View Of Crypto As National Security Threat

By **Katherine Kirkpatrick, Christine Savage, Russell Johnston and Sumon Dantiki**
March 18, 2020, 6:27 PM EDT


Katherine Kirkpatrick


Christine Savage


Russell Johnston


Sumon Dantiki

In the past, sanctioned jurisdictions like Venezuela have embraced virtual currency as a way to bypass channels that involve U.S. dollars, blunting the impact of U.S. economic sanctions policies aimed at isolating those countries from the U.S. financial system.

U.S. regulators have moved quickly to limit loopholes that could make unusable certain aspects of cryptocurrencies well suited to evade enforcement.[1]

In addition to nation-states using virtual currencies to evade sanctions, terrorist groups have shown an interest in using them to finance operations, and transnational criminal organizations use cryptocurrencies to facilitate money laundering.

In his final redacted report, former Special Counsel Robert Mueller likewise noted that subunits of the General Staff of the Russian Army used "a bitcoin mining operation to secure bitcoins used to purchase computer infrastructure used in [2016 foreign influence] hacking operations."[2]

More recently, the National Security Agency has also publicly highlighted that cryptocurrency continues to be an enabler of foreign influence operations.[3]

In recent days, U.S. authorities have taken significant coordinated actions to address the illicit use of cryptocurrency to evade sanctions and other legal prohibitions, as well as to target the underlying infrastructure used to do so — and have signaled their resolve to do even more.

On March 2, the U.S. Department of the Treasury's Office of Foreign Assets Control and the U.S. Department of Justice announced parallel actions to address violations by two Chinese nationals involved in laundering over $100 million worth of stolen cryptocurrency from a cyber intrusion linked to North Korea against a cryptocurrency exchange in 2018.

OFAC sanctioned the two Chinese nationals, while the DOJ and several investigative agencies — the Federal Bureau of Investigation, the Internal Revenue Service, and

Homeland Security Investigations — jointly announced both a criminal indictment and a civil forfeiture complaint against the same individuals for laundering over $100 million worth of virtual currency.[4]

Similarly, the DOJ has recently signaled its intent to investigate and prosecute technical and human facilitators of illicit activities facilitated by cryptocurrency. In February, for instance, the DOJ indicted a U.S. national who operated Helix, a bitcoin mixer service designed to allow users to send bitcoin in a manner that concealed the source or owner of the bitcoin.

And in January, the DOJ indicted Ethereum developer Virgil Griffith with conspiracy to violate the International Emergency Economic Powers Act after he traveled to North Korea to attend the Pyongyang Blockchain and Cryptocurrency Conference, where he allegedly discussed "how blockchain and cryptocurrency technology could be used by North Korea to launder money and evade sanctions, and how the [Democratic People's Republic of Korea] could use these technologies to achieve independence from the global banking system."[5]

Pursuit by enforcement agencies and awareness of the potential evasive use of cryptocurrency, however, has not stifled creative attempts to manipulate the U.S. sanctions regime or evade criminal laws — with a notable uptick in actions by U.S. government regulators and law enforcement authorities.

In a recently released report, one leading cryptocurrency exchange reported a 49% increase in global law enforcement requests (with over 60% originating from U.S. law enforcement agencies) in 2019 as compared to 2018.[6] For their part, a broad array of U.S. law enforcement agencies are both placing greater internal emphasis on the misuse of virtual currencies and requesting additional resources to address them.[7]

In its 2021 budget request, for example, the IRS asked for funds to "support the hiring of 108 special agents to conduct more criminal investigations related to cyber and virtual currency."[8]

Here we briefly examine efforts in certain sanctioned jurisdictions to use cryptocurrencies to evade sanctions. We also discuss what efforts businesses can take to limit exposure to cryptocurrency sanctions and growing federal investigative agency demands.

North Korea

On Feb. 9, cybersecurity company Recorded Future, which specializes in threat intelligence, released a report indicating that North Korea appears to be increasing efforts to mine and embrace cryptocurrency in an effort to evade sanctions.[9] Indeed, later that month, on February 22-29, North Korea was set to hold its second cryptocurrency conference.

The first conference, in April 2019, allegedly included "explicit discussion of cryptocurrency for sanctions evasion and money laundering."[10] Leading up to the second conference, United Nations sanctions experts explicitly warned people to stay far afield from the conference, indicating that attendance alone may be considered a violation of sanctions.[11]

The U.N.'s focus on North Korea includes tracking the jurisdiction's crypto criminal efforts. For example, a recent U.N. report indicated that North Korea has generated billions in cyberattacks targeting banks and cryptocurrency exchanges.[12] In the report, the U.N. experts said North Korea's attacks against cryptocurrency exchanges allowed it "to generate income in ways that are harder to trace and subject to less government oversight and regulation than the traditional banking sector."[13]

The U.N. also accused North Korea of using a Hong Kong-based blockchain firm as a front to launder money. The committee found that the blockchain-based shipping and logistics firm was founded by North Korean state actors as a shell company, and the funds were originally sourced from online extortion efforts that demanded payment in cryptocurrency.[14]

The U.N. described detailed, complicated efforts by North Korea to conceal the criminal activity — namely, a method of manipulation that creates thousands of layered transactions through single use cryptocurrency wallets. In fact, the U.N. cited one transaction where stolen funds were transferred through thousands of separate transactions and routed to multiple countries before finally converting the crypto to fiat currency.[15]

The focus on North Korea's illegal use of cryptocurrency has not been limited to the U.N. For example, OFAC's designation of two Chinese nationals on March 2 for their role in laundering stolen cryptocurrency linked to a North Korean state-sponsored malicious cyber group's 2018 cyber intrusion was accompanied by a lengthy press release describing the history of North Korea's "malicious cyber-enabled activities."[16]

OFAC's release quotes U.N. numbers to prove that "North Korea's malicious cyber activity is a key revenue generator for the regime, from the theft of fiat currency at conventional financial institutions to cyber intrusions targeting cryptocurrency exchanges."[17]

Likewise, the Department of Justice indicted the same two Chinese nationals and filed civil forfeiture complaints to seize over $100 million in stolen revenue generated by the theft of cryptocurrency.[18]

In 2018, DOJ also unsealed charges against Park Jin Hyuk, a North Korean national accused of cybercrimes against virtual currency exchanges worldwide and assisting with several international cyberattacks such as the 2017 WannaCry 2.0 global ransomware attack, the 2016 theft of $81 million from Bangladesh Bank, and the 2014 attack on Sony Pictures Entertainment Inc.[19]

North Korea's pattern of stealing cryptocurrency has expanded to mining cryptocurrency, and all indications point to the country's continued interest in and use of cryptocurrency. Similar to Venezuela's attempt to use the Petro, a state-backed cryptocurrency launched in February 2018 (and quickly muffled by sanctions), North Korea has significantly increased its mining of a privacy-oriented currency called Monero, which hides transaction information and makes the flow of money difficult to trace.[20]

The troublesome use of Monero was first discovered in 2018, when cybersecurity researchers at AlienVault LLC found evidence of malware that infected computers to mine Monero and send it back to Kim Il Sung University in Pyongyang.[21]

Iran

The U.S. Department of the Treasury and the U.S. Department of Justice are well aware of Iran's continued interest in cryptocurrency and has reacted to tamp down efforts by individuals in that jurisdiction attempting to skirt sanctions.

In November 2018, for example, DOJ unsealed criminal indictments against Iranian individuals who deployed ransomware against over 200 targets (including hospitals, the Port of San Diego, and the cities of Atlanta and Newark) to collect ransoms in virtual currencies in coordination with OFAC which, for the

first time, imposed sanctions on two Iranians who then helped exchange those Bitcoin ransom payments into Iranian rial.[22]

Iran continues to embrace crypto, however, even in the face of some adverse developments — both enforcement and otherwise. For example, in June 2019, Iran's power grid was hit by a massive, crypto mining induced power surge, which led the Iran Ministry of Energy to declare that power to miners would be cut off. But mere months later, Iran officially recognized crypto mining as a legal sector in the economy.

Cryptocurrency developers in Iran have also publicly and successfully circumvented U.S. sanctions using cryptocurrency — albeit for humanitarian purposes. Volunteer developers established IranRescueBit, where people can make crypto donations to help victims of Iran's devastating floods in the spring of 2019. By using crypto, donors have sidestepped sanctions that have allegedly prohibited other international donations to Iranian nongovernmental organization.[23]

IranRescueBit directors have said they intend to convert the crypto donations to fiat using local exchanges, and then send that currency to Iranian-based humanitarian organizations. Thus, although the intent is good, the implication is clear—crypto can and is currently being used to circumvent sanctions.

Iran is also benefiting from coordination with other jurisdictions. In 2017, the Swedish government allowed a blockchain startup, Brave New World Investments AB, to use a bitcoin account to trade in equities on the Tehran Stock Exchange.[24] The startup was initially blocked by Swedish banks because of the potential implications for their U.S. operations.

In 2018, Iranian and Russian blockchain industry participants agreed to cooperate in developing Iran's blockchain industry, with a specific nod to addressing challenges arising from sanctions.[25] In 2019, Iran's Trade Promotion Organization held talks with eight countries to "start ... a new chapter in its international monetary transactions to circumvent U.S.-led sanctions," by using cryptocurrency.[26]

Finally, speculation abounds that Iran's lack of military might could be counteracted by an onslaught of cyber aggression and embrace of digital currency in economically-driven efforts, which is supported by the fact that Iranians began buying Bitcoin at a premium shortly after the January 2020 tensions between the U.S. and Iran escalated.[27]

Defensive Efforts and Compliance

The potential misuse of cryptocurrency to avoid sanctions is worrisome for entities striving for compliance, but still struggling to ramp up to understand the many facets of this asset class.

As a starting point, the U.N. has recommended the following: (1) member states should regulate cryptocurrency exchanges; (2) cryptocurrency exchanges should expand their current AML obligations to meet the same standards as banks; and (3) financial institutions should take independent steps to protect against North Korean cyber activities.

For compliance-oriented financial services entities, particularly those that deal closely with digital assets, knowing how to tailor a compliance program to operate successfully in this space can be tricky. As technology increases, and national security risks within the crypto ecosystem, including foreign nations

who engage in activities such as mining and training younger developers, financial services entities should consider employing the following standards:

- Creating a dialogue with law enforcement and regulatory agencies on threat actors, methods and patterns;

- Adhering to strict know-your-customer measures for all users, including enhanced due diligence where warranted;

- Implementing reasonable anti-money laundering procedures including transaction monitoring, detection, and suspicious activity reporting;

- Deploying pattern assessment, particularly with transfers involving external, unhosted wallets, along with potentially limiting such transfers or increasing scrutiny of them;

- Assessing geographic risk exposure, such as identifying those transactions in proximity to or affiliated with a sanctioned jurisdiction;

- Understanding and continuously aggregating cryptocurrency-specific red flags for use in monitoring transactions and personnel;[28]

- Understanding evolving risks, including new crypto users, sanctioned or suspicious addresses, darknet websites, and shell websites;

- Maintaining proactive communication with regulators after attacks and/or any kind of exposure, and taking immediate steps to prevent or contain the damage (e.g., freezing assets of sanctioned entities and blocking related malicious transactions);

- Using a feedback loop to analyze data, suspicious activity, breaches, and other meaningful events to refine the program over time;

- Maintaining robust documentation of issues and incidents and providing adequate and continuing training to relevant staff;

- Considering the use of filters that go beyond checking whether specific addresses are on sanctions lists, as parties may control other addresses within the same wallet. Similarly, ideally funds would be traced through the blockchain to be sure there was no interaction with sanctioned addresses or addresses from sanctioned jurisdictions;[29] and

- Implementing rigorous and continuous methods of identifying parties who have transacted, or are transacting, with sanctioned entities.[30]

For preventing state-run activities, cryptocurrency exchanges or other similar participants should consider added financial intelligence, which would include personnel with specific training in criminal investigations or intelligence.

They should know — or find out before facilitating a transaction — whether and why their customers are using cryptocurrency, particularly if cryptocurrency supports an underlying aspect of the business (e.g., website maintenance) so the exchange can help appropriately identify monetary flows.

Reviewing prior law enforcement or regulatory legal process or requests for information and identifying any challenges form cryptocurrency use.

Guidance from the Financial Action Task Force and the Financial Crimes Enforcement Network has expanded the application of the Travel Rule, an anti-money laundering obligation, to virtual currency, and these expanded requirements go into effect in June.[31]
These rules would mandate the application of many of the recommendations listed above. In addition, the growing interest by federal investigative agencies and prosecutors in illicit use of cryptocurrencies — and overt coordination with the Department of Treasury — signals that many of the recommendations outlined in the Travel Rule may become a de facto set of requirements across the federal government.

But the inherent differences between conventional platforms and cryptocurrency platforms, especially in light of the pseudonymous nature of wallet addresses, makes compliance with such recommendations exceptionally challenging for Financial Services clients who deal with virtual currency.

Thus, crypto participants must grapple with potential solutions to best implement compliance protocols that will both practically ensure the security of their assets, the legality of their operations, and compliance with relevant regulatory requirements.

Katherine Kirkpatrick, Christine Savage, Russell Johnston and Sumon Dantiki are partners at King & Spalding LLP.

[1] King & Spalding Client Alert, Virtual Currency in Sanctioned Jurisdictions (Feb. 19, 2019).

[2] Rep. on the Investigation Into Russian Interference In the 2016 Presidential Election (Vol. I) at 36-37 (Mar. 2019), available at https://www.justice.gov/storage/report.pdf.

[3] Fazzani, Kate, Foreign election trolls continue to gain traction, fueled by cryptocurrencies and the sale of 'influence packages' online: NSA cyber lead, CNBC (Jul. 23, 2019), https://www.cnbc.com/2019/07/23/nsa-says-election-trolls-gaining-traction.html.

[4] Press Release, OFAC, Treasury Sanctions Individuals Laundering Cryptocurrency for Lazarus Group (Mar. 2, 2020), available at https://home.treasury.gov/news/press-releases/sm924; Press Release, United States Department of Justice, Two Chinese Nationals Charged with Laundering over $100 million in Cryptocurency From Exchange Hack (Mar. 2, 2020), available at https://www.justice.gov/opa/pr/two-chinese-nationals-charged-laundering-over-100-million-cryptocurrency-exchange-hack.

[5] Complaint at 6, U.S. v. Griffith, No. 19 MAG 10987 (S.D.N.Y. Nov. 21, 2019), available at https://www.justice.gov/usao-sdny/press-release/file/1222646/download.

[6] Khatri, Yogita, Kraken received 50% more regulatory inquiries last year, Yahoo Finance (Jan. 7, 2020), https://finance.yahoo.com/news/kraken-received-50-more-regulatory-070013146.html.

[7] Rosenstein, Phillip, White House Sets Sights on Crypto Threats in 2021 Budget, (Feb. 10, 2020) Law360, https://www.law360.com/articles/1242532/white-house-sets-sights-on-crypto-threats-in-2021-budget; Foxley, William, FBI Director: Cryptocurrency is a 'Significant Issue' for Law Enforcement, Yahoo Finance (Nov. 8, 2019) (cryptocurrency challenges likely to get "bigger and bigger"), https://finance.yahoo.com/news/fbi-director-cryptocurrency-significant-issue-121331175.html.

[8] IRS, Congressional Budget Justification & Annual Performance Report and Plan: Fiscal Year 2021, at 125, https://home.treasury.gov/system/files/266/02.-IRS-FY-2021-CJ.pdf.

[9] Recorded Future Report, How North Korea Revolutionized the Internet as a Tool for Rogue Regimes (2020), https://go.recordedfuture.com/hubfs/reports/cta-2020-0209.pdf.

[10] Michelle Nichols, Exclusive: U.N. sanctions experts warn - stay away from North Korea cryptocurrency conference, Reuters (Jan. 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.

[11] After the United Nations issued its warning, publicly available information from conference organizations was removed from the internet, and it is unclear whether the conference ultimately took place.

[12] Rep. of the Panel of Experts, 74th Sess., Aug. 30, 2019, U.N. Doc. S/2019/691, available at https://undocs.org/S/2019/691.

[13] Id., at 4.

[14] Id., at 29.

[15] Id., at 27.

[16] Press Release, OFAC, Treasury Sanctions Individuals Laundering Cryptocurrency for Lazarus Group (Mar. 2, 2020), available at https://home.treasury.gov/news/press-releases/sm924.

[17] Id.

[18] Press Release, United States Department of Justice, Two Chinese Nationals Charged with Laundering over $100 million in Cryptocurency From Exchange Hack (Mar. 2, 2020), available at https://www.justice.gov/opa/pr/two-chinese-nationals-charged-laundering-over-100-million-cryptocurrency-exchange-hack.

[19] Press Release, North Korean Regime-Backed Programmer Charged With Conspiracy to Conduct Multiple Cyber Attacks and Intrusions (Sept. 6, 2018), https://www.justice.gov/opa/pr/north-korean-regime-backed-programmer-charged-conspiracy-conduct-multiple-cyber-attacks-and.

[20] Mike Orcutt, North Korea Appears to Have Expanded its Crypto-Mining Operation MIT TECHNOLOGY REVIEW (Feb. 11, 2020), https://www.technologyreview.com/f/615177/north-korea-cryptocurrency-mining-monero/.

[21] Rjun Kharpal, What You Should Know About North Korea's New Favorite Cryptocurrency, CNBC (Jan. 10, 2020), https://www.cnbc.com/2018/01/10/what-is-monero-north-korea-new-favorite-cryptocurrency.html.

[22] Press Release, U.S. Dep't of Justice, Two Iranian Men Indicted for Deploying Ransomware to Extort Hospitals, Municipalities, and Public Institutions, Causing Over $30 Million in Losses (Nov. 28, 2018), available at https://www.justice.gov/opa/pr/two-iranian-men-indicted-deploying-ransomware-extort-hospitals-municipalities-and-public; Press Release, U.S. Dep't of Treasury, Treasury Designates Iran-Based Financial Facilitators of Malicious Cyber Activity and for the First Time Identifies Associated Digital Currency Addresses (Nov. 28, 2018), available at https://home.treasury.gov/news/press-releases/sm556.

[23] For example, according to the Iranian Red Crescent Society, US sanctions have impeded relief efforts through blocking foreign financial aid. CipherTrace Report, Q3 2019 Cryptocurrency Anti-Money Laundering Report (2019), https://ciphertrace.com/q3-2019-cryptocurrency-anti-money-laundering-report/.

[24] Avi Mizrahi, New Swedish Firm Offers Iranian Stock Investment for Bitcoin, FINANCE MAGNATES (Mar. 24, 2017), https://www.financemagnates.com/cryptocurrency/news/new-swedish-firm-offers-iranian-stock-investment-bitcoin/.

[25] Lubomir Tassev, Russian Developers to Help Iran Build Its Crypto-Economy, BITCOIN,COM (Nov. 14, 2018), https://news.bitcoin.com/russian-developers-to-help-iran-build-its-crypto-economy/.

[26] Talks With 8 Countries Over Using Cryptocurrency in Monetary Transactions Going On, TEHRAN TIMES (Jan. 28, 2019), available at https://www.tehrantimes.com/news/432400/Talks-with-8-countries-over-using-cryptocurrency-in-monetary.

[27] Tony Spilotro, Are Iranians Buying Bitcoin at Premium in Anticipation of War, NEWSBTC (Jan. 3, 2020), https://www.newsbtc.com/2020/01/03/are-iranians-buying-bitcoin-at-premium-in-anticipation-of-war/.

[28] For example, personnel should identify customers associated with advertisements for cryptocurrency trading on sites available to users in sanctioned jurisdictions. Personnel should also understand that they need to question customers dealing with exchanges associated with or close to sanctioned jurisdictions where there is no logical (and documented) explanation.

[29] A user can pass funds through multiple wallets before sending them to a financial institution, but this activity is often visible and can be monitored through third party software solutions.

[30] For example, when Venezuela initially launched the Petro, it approved sixteen cryptocurrency exchanges to handle transactions. An organization may want to identify and prohibit transactions with those exchanges.

[31] King & Spalding Client Alert, Fake It Till You Make It: The Travel Rule And Virtual Currencies (Oct. 1, 2019), https://www.kslaw.com/news-and-insights/fake-it-till-you-make-it-the-travel-rule-and-virtual-currencies.