Crypto evasion: The new frontier of sanctions enforcement

The United States Department of Justice ("DOJ") recently brought criminal charges in a first-of-its-kind prosecution against a US citizen for allegedly transmitting more than $10 million in bitcoin to a sanctioned country to evade US law. On 13 May 2022, US Magistrate Judge Zia Faruqui, a former national security prosecutor, released an unusual opinion explaining why he had approved the first cryptocurrency sanctions complaint, which remains under seal.[1] As a result, the opinion did not disclose the name of the defendant, the identities of the virtual currency exchanges used, or the sanctioned country at issue.[2] Judge Faruqui's opinion dispelled any uncertainty about the viability of criminally prosecuting individuals involved in transferring virtual money such as Bitcoin, Ethereum or Tether, created outside the traditional financial system, to sanctioned countries, entities, or individuals. Accordingly, those transactions may form the basis for both civil and criminal liability.

What is cryptocurrency?

Cryptocurrency is a digital asset that makes it possible to transfer value online without using a bank or payment processor. For example, Bitcoin, the most popular virtual currency, allows two people to cheaply and quickly transfer money anywhere in the world, simply with an internet connection. Unlike US dollars, cryptocurrency is not backed by a government and the values change constantly. Cryptocurrency can be purchased through an exchange, app on your phone, on a website, or a cryptocurrency ATM. A digital wallet (usually a long string of random numbers and letters) is necessary to send, receive, and store cryptocurrency.

> In March 2022, the US Department of Justice launched the KleptoCapture Task Force to prosecute any person or entity involved in violating the Russian sanctions and seize their assets.

Because cryptocurrency is encrypted and decentralized, it offers the illusion that transactions are anonymous and not traceable. As a result, crypto has been used for illicit purposes from financing criminal activities to ransom payments for cyberextortion. Cryptocurrency transactions, however, are recorded on a public ledger called a "blockchain" that can be used to identify the buyers and sellers in transactions using blockchain analysis software.

Sanctions evasion

After the United States, European Union, and other countries imposed comprehensive sanctions against Russia for its unprovoked and horrific invasion of Ukraine, world leaders expressed concern that cryptocurrencies could be used to evade sanctions. Crypto-currencies make up a greater part of Russia's financial system than any other nation due to distrust of its banking systems. Ukraine requested crypto exchanges, including Coinbase and Binance, the two largest in the world, impose a blanket ban on Russian users. Coinbase and Binance refused this request, but agreed to block any accounts or transactions suspected to involve a sanctioned individual or entity.

In March 2022, DOJ launched the KleptoCapture Task Force to prosecute any person or entity involved in violating the Russian sanctions and seize their assets. One of the task force's primary goals is to target "efforts to use cryptocurrency to evade US sanctions." The task force will be assisted by DOJ's National Cryptocurrency Enforcement Team.

Reprinted with permission from the July/August 2022 issue of Export Compliance Manager.
www.exportcompliancemanager.com

First cryptocurrency sanctions case

In or around May 2022, DOJ filed an application for a criminal complaint with Judge Faruqui charging a US person ("Defendant") with conspiring to violate the International Emergency Economic Powers Act ("IEEPA"), 50 USC. § 1705, and defrauding the United States, in violation of 18 USC. § 371. IEEPA makes it illegal to violate comprehensive trade-based sanctions programs (e.g., Iran, North Korea, and Russia) administered by the Treasury's Office of Foreign Assets Control ("OFAC") and carries a stiff maximum penalty – 20 years' imprisonment and a $1,000,000 fine. Most sanction regimes "prohibit the direct and indirect importation, exportation, and re-exportation of goods, services, and technology, without a license from OFAC."

Judge Faruqui concluded that there was probable cause to believe the Defendant, using virtual currency exchanges in the US and a foreign country, sent more than $10 million worth of bitcoin to the sanctioned country for customers of a Paypal-type payment platform system the Defendant assisted in creating in the sanctioned country. The Defendant proudly marketed the payment platform as a way to evade sanctions and didn't hide his illegal activity. Investigators uncovered this scheme using subpoena returns from virtual currency exchanges (including the account access logs), email search warrant returns, and banking information.

There are two important takeaways from this case. First, virtual currency is traceable; cryptocurrency's reputation for anonymity is a myth. Second, US sanctions apply to transactions involving virtual currencies the same way as those involving traditional fiat currencies.

OFAC's crypto enforcement actions

OFAC's sanctions prohibit US companies from engaging in transactions with, or providing financial services to, sanctioned countries or specially designated nationals and blocked persons. Additionally, because the standard for civil liability for violating economic sanctions is strict liability, companies face severe civil penalties even if there is no negligence, intent, or other finding of fault.

OFAC has found companies liable for sanctions violations stemming from deficient internal controls and screening procedures, reaching large civil settlements with several cryptocurrency service providers. In December 2020, OFAC fined BitGo $98,830.00, and in February 2021, OFAC reached a $507,373 settlement with Bitpay for over 2,000 alleged cryptocurrency sanctions violations.

In September and November 2021, OFAC designated two virtual currency exchanges, Suex and Chatex, for facilitating financial transactions for ransomware actors. In April 2022, in coordination with the German government's seizure of $25 million of Bitcoin, OFAC sanctioned the world's largest darknet market, Hydra Market, for offering illegal services through its Russian-based site.

Most recently, in May, OFAC issued its first sanctions against a cryptocurrency "mixer," Blender.io, which was used by the Lazarus group, a group sponsored by North Korea's government, to launder $20.5 million of cryptocurrency to support illicit activities.

Follow the guidance

Companies should review and update their compliance programs to avoid unknowingly assisting in the evasion of US sanctions.[3] Listed below are tips that should be considered when using cryptocurrency.

Transaction screening and monitoring

Crypto transactions should be screened and monitored to identify all pertinent information concerning virtual currency addresses, which may be linked to sanctioned persons or jurisdictions. Incorporate geolocation tools, IP misattribution controls, and transaction monitoring and investigation in your compliance program.

Know Your Customer procedures

Use Know Your Customer ("KYC") procedures to obtain information about customers and use that information to conduct due diligence to reduce potential sanctions-related risks. This includes collecting not only basic identifying information such as legal name, date of birth/incorporation, physical and email addresses, nationality, but also IP addresses associated with transactions and logins, bank information, corporate ownership information, identification/residency documents or information about where an entity conducts its business.

Red flags

Be on the lookout for red flags such as customers who:

- provide inaccurate or incomplete KYC information;
- are non-responsive or refuse to provide KYC information;
- attempt to access your company's website, online portals, or services from an IP address or VPN connected to a sanctioned jurisdiction; or
- attempt making payment using a digital wallet or virtual currency address associated with a blocked person or sanctioned jurisdiction.

If you discover your company may have violated OFAC's sanctions, consider making a voluntary self-disclosure to DOJ and OFAC in order to mitigate potential liability.

Conclusion

Failure to comply with OFAC sanctions can bring harsh criminal and civil penalties for companies for sanctions violations involving cryptocurrency. ■

About the authors:

B. Stephanie Siegmann is a Partner at the law firm of Hinckley, Allen & Snyder LLP, and Chair of its International Trade and Global Security Practice. Prior to joining Hinckley Allen, Stephanie served as the National Security Chief at the U.S. Attorney's Office for the District of Massachusetts and worked as both a federal and Navy JAG prosecutor for more than 22 years.

Isha Kumar is a student at Boston University School of Law and is working as a summer associate at Hinckley Allen.

www.hinckleyallen.com

[1] In re: Criminal Complaint, No. 22-mj-00067, 2022 WL 1573361 (D.D.C. May 13, 2022).
[2] A complaint is typically unsealed upon the defendant's arrest, but may remain sealed even after arrest, if the defendant is cooperating with DOJ.
[3] See OFAC Guidance available at http://home.treasury.gov/system/files/126/virtual_currency_guidance_brochure.pdf.