CADWALADER

Cabinet **News and Views**

Informed analysis for the financial services industry

In Depth: Listen to Your Regulator on Sanctions and Crypto

By **James A. Treanor**
Special Counsel | White Collar Defense and Investigations

It should come as no surprise that the crushing sanctions imposed on Russia in recent weeks will be met with efforts to evade their impact. From Russian firms starved for U.S. dollars to oligarchs starved for that new villa or yacht, some sanctions targets inevitably will attempt to access the capital, goods and services from which they have been severed so completely since Russia's invasion of Ukraine began. To do so, in most cases they will be forced to conceal their involvement in a transaction. Enter: crypto.

Almost immediately after the conflict erupted, concerns were raised by pundits and policymakers that cryptocurrencies – by virtue of their decentralization and the anonymity they afford – could turbocharge efforts to evade the massive package of sanctions imposed on Russia. For example, in a March 2 letter, Senators Elizabeth Warren and Mark Warner wrote to Secretary of the Treasury Janet Yellen asking for information on how Treasury intends to "inhibit the use of cryptocurrency for sanctions evasion."

In response to these alarm bells, industry experts have observed that, in fact, digital currencies are unsuitable to sanctions evasion. For starters, crypto is arguably too small to accommodate widespread sanctions evasion – that is, there is simply not enough cryptocurrency available to facilitate the systematic evasion of sanctions against a country like Russia, which has the world's eleventh largest economy.

In addition, sanctions evasion, like other forms of money laundering, demands obscurity and non-traceability. Cryptocurrency – for all the talk of anonymity and decentralization – has transparency and traceability literally built into its DNA. A blockchain is, after all, a public and immutable record of all transactions. Even if identities are not attached to those transactions, authorities are increasingly adept at putting names and faces to the blockchain's ones and zeroes. Witness the DOJ and FBI's successful effort to recover millions of dollars in bitcoin ransomware

payments, and the arrest of two New York residents who stole and unsuccessfully attempted to launder approximately $4.5 billion in cryptocurrency.

These arguments against cryptocurrency as an effective tool of sanctions evasion undoubtedly have merit. But for exchangers, administrators, wallet providers, and others involved in the industry, they risk missing the point. First, there is little doubt that cryptocurrency can be – indeed, has been – used to evade sanctions, even if not on a massive scale. More importantly, the U.S. government has in recent months repeatedly highlighted legal risks associated with cryptocurrency, including in connection with sanctions evasion. Last fall, OFAC released some of its most detailed compliance guidance ever, devoted entirely to sanctions risks in the cryptocurrency industry. The following month, in its anticipated Sanctions Review, one of Treasury's central messages was that cryptocurrencies and other technologies may provide bad actors with "new ways of hiding cross-border transactions" and thereby "reduce the efficacy of American sanctions."

More recently, on March 1 – soon after large-scale Russian military action began – President Joseph R. Biden announced in his State of the Union Address the formation of a DOJ-led initiative "to go after the crimes of Russian oligarchs." In an announcement released the following day, DOJ made clear that one mission of the new "KleptoCapture" task force would be to target "efforts to use cryptocurrency to evade U.S. sanctions." Most recently, FinCEN warned financial institutions on March 7 to "be vigilant about potential Russian sanctions evasion, including by both state actors and oligarchs." The notice also underscored that "CVC [convertible virtual currency] exchangers and administrators and other financial institutions may observe attempted or completed transactions tied to CVC wallets or other CVC activity associated with sanctioned Russian, Belarusian, and other affiliated persons." And most recently, President Biden's March 9 Executive Order underscores that understanding and managing the potential threats posed by cryptocurrency will be an all-of-government effort, and a key area of focus for the administration going forward.

The clear message, then, is that regardless of the actual viability of cryptocurrency as a means of evading sanctions, OFAC, DOJ, FinCEN, and other enforcement agencies will be looking hard for violations. Whether many or few, the U.S. Government will find violations, and those involved – including financial institutions, exchangers, wallet providers, and other market participants – will be held accountable. Firms that do not heed their regulators' repeated warnings to understand the risk environment, appropriately diligence users, and implement other suitable controls may soon regret it.