Proskauer

Economic Sanctions and Asset Seizures: An Important Focus for the Biden Administration

The Capital Commitment Blog on **March 9, 2022**

Sanctions continue to be a dynamic area of regulation and enforcement. In its first year, the Biden Administration has already undertaken a number of different sanctions initiatives. The three examples below highlight the range of strategies employed and their potential ramifications for private investment funds.

(1) Sanctions on Russia over Ukraine

In response to Russia's actions in Ukraine, the U.S. has ramped up economic pressure by imposing sweeping sanctions on major Russian financial-institutions, Russian oligarchs, and members of Russian President Vladimir Putin's inner circle, and even Putin himself. The Department of Treasury's Office of Foreign Assets Control ("OFAC") has also expanded restrictions on trading Russian sovereign debt and transactions involving debt and equity, and restricted the ability of U.S. financial institutions to clear transactions with certain Russian banks. The U.S. has also imposed sanctions that in the past it has disfavored, including removing some Russian banks from the SWIFT financial messaging system and imposing sanctions on the company in charge of building Russia's Nord Stream 2 gas pipeline designed to double gas flow capacity between Russia and Germany.

Alongside sanctions, the Department of Justice recently announced a new task force, "KleptoCapture," focused on seizing assets belonging to sanctioned persons and criminal actors, and specifically targeting the crimes of Russian oligarchs and those who aid or conceal their unlawful conduct.

Circumstances have changed since 2014 when the U.S. and its western allies imposed sanctions after Russia seized Ukraine's Crimean Peninsula. Since then, Putin has built up Russia's international reserves, reduced its public debt, and increased trade deals with non-European countries like China. Meanwhile, Europe has grown increasingly dependent on Russia for its energy needs. As a result, some speculate that U.S. sanctions may have less of an impact on Russia's economy, and sanctions on Russia's energy sector are likely to have significant repercussions for European allies. However, the expanded sanctions against Russia are already having a dramatic effect on Russia's ability to participate in the global economy.

Moreover, regulators are anticipating the possibility that Russia may try to evade sanctions through the use of cryptocurrencies. For example, Russia could conduct ransomware attacks to steal cryptocurrency and could find people or entities willing to trade in cryptocurrency, which it could do outside of the international banking system. Accordingly, Task Force KleptoCapture is also focused on this space.

(2) Sanctions in the Virtual Currency Space

Sanctions developments in the digital assets space are especially important given the growing threat that ransomware poses to the public and the economy. In response to this threat, OFAC has ramped up its efforts to fight ransomware payments.

In recent years, OFAC sanctions have increasingly targeted individuals and entities who have used virtual currency in connection with criminal activity. For example, in 2021, OFAC entered into a $500,000 plus settlement with BitPay, Inc., a cryptocurrency payment processing platform, for allowing persons in sanctioned jurisdictions to engage in digital currency-related transactions with BitPay's merchant customers in violation of multiple sanctions.

OFAC has also sanctioned the virtual currency exchanges themselves. In September 2021, OFAC placed a Russian-based virtual currency exchange (SUEX) on its Specially Designated Nationals and Blocked Persons List ("SDN List") for facilitating financial transactions for ransomware actors. In November 2021, OFAC sanctioned another virtual currency exchange, Chatex for its facilitation of ransomware payments.

OFAC can bring enforcement actions and impose penalties for sanctions violations based on strict liability, meaning that a U.S. person or entity can be deemed to have violated U.S. sanctions without having knowledge or reason to know it was engaging in a transaction prohibited under sanctions laws and regulations.

OFAC has discouraged U.S. companies from making ransomware payments and issued guidance warning companies that given the strict liability standard they could face consequences for making a ransom payment to a hacker that turned out to be a sanctioned entity, even if they were not aware of the hacker's identity at the time of the payment. However, OFAC has indicated it will consider the totality of facts and circumstances surrounding the violation before imposing liability. Important mitigating factors include the company's implementation of measures to prevent and protect against attacks, and reporting the attack to the appropriate government agency.

(3) Sanctions and Anti-Corruption Enforcement

The Global Magnitsky Human Rights Accountability Act authorizes the US government to impose sanctions on those it deems to be human rights abusers and corrupt government officials. An individual or entity sanctioned under this Act can be included in the SDN List. As a result of this designation, all of their property and interests in property within U.S. jurisdictions are blocked and U.S. persons are generally prohibited from engaging in transactions with them. OFAC has also clarified that these sanctions apply to entities whose majority owner is a sanctioned individual or entity.

This is especially concerning for entities or persons engaged in international transactions. Private investment funds, especially those who made investments in and draw investors from foreign countries, must be extra vigilant and closely follow OFAC's Framework for OFAC Compliance Commitments. OFAC has consistently made clear that companies facilitating or engaging in online commerce or companies processing transactions using digital currency are responsible for ensuring that they do not engage in transactions prohibited by OFAC sanctions.

Because the Global Magnitsky Act designates corrupt actors as SDNs, it can potentially open another avenue for the government to bring corruption cases. This is important because, given that strict liability applies to sanctions violations, the use of the Global Magnitsky sanctions program to prosecute corruption cases effectively lowers the government's evidentiary burden. In other words, instead of proving intentional violations of the Foreign Corrupt Practices Act (FCPA) and other anti-corruption statutes, prosecutors and regulators could potentially bring actions based on an underlying sanctions violation for which a company can be held strictly liable.

Read more of our Top Ten Regulatory and Litigation Risks for Private Funds in 2022.

View Original

Related Professionals

- **Steven Baker**
  Partner
- **Margaret A. Dale**
  Partner
- **Mike Hackett**
  Partner
- **William C. Komaroff**
  Partner
- **Timothy W. Mungovan**
  Chairman of the Firm
- **Dorothy Murray**
  Partner
- **Joshua M. Newville**
  Partner
- **Todd J. Ohlms**
  Partner
- **Seetha Ramachandran**
  Partner
- **Jonathan M. Weiss**

Partner

- **Julia D. Alonzo**
  Senior Counsel
- **James Anderson**
  Senior Counsel
- **Julia M. Ansanelli**
  Associate
- **William D. Dalsen**
  Senior Counsel
- **Adam L. Deming**
  Associate
- **Reut N. Samuels**
  Associate
- **Hena M. Vora**
  Associate