Economic sanctions and export control considerations when facing a ransomware attack

By Anthony Rapa, Esq., Carrie Schroll, Esq., and Sunil Shenoi, Esq., Kirkland & Ellis LLP

DECEMBER 16, 2021

On Sept. 21, 2021, in response to a substantial increase in ransomware attacks against sensitive targets such as major pipeline systems, state and local governments, and insurance carriers, the U.S. Department of the Treasury's Office of Foreign Assets Control ("OFAC") issued (https://bit.ly/3iXJJLt) an "Updated Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments" (the "Advisory") highlighting the need to consider sanctions compliance when addressing ransomware attacks.

The Advisory makes clear that making or facilitating cyber ransom payments to persons with a sanctions nexus can violate U.S. sanctions.

As described below, companies facing a ransomware attack, or in the process of developing a ransomware attack response plan as recommended in the Advisory, should seek to adequately address sanctions compliance, as well as export controls compliance.

Sanctions and export controls risks related to ransomware attacks

The Advisory makes clear that making or facilitating cyber ransom payments to persons with a sanctions nexus can violate U.S. sanctions. In particular, entities risk sanctions violations if ransom payments are made directly or indirectly to sanctioned persons, such as those on OFAC's List of Specially Designated Nationals or Blocked Persons ("SDN List"), or to persons in comprehensively sanctioned jurisdictions, such as Cuba, Iran, North Korea, Syria, or the Crimea region.

Determining whether payment to a perpetrator violates U.S. sanctions can pose significant compliance challenges, as companies often will not know where a perpetrator is located. Even under such circumstances, however, OFAC still can impose strict liability for ransomware payments to sanctioned countries or persons and expects companies to attempt to identify any sanctions nexus through screening and geolocation tools.

Under its cyber-related sanctions program, OFAC already has designated (https://bit.ly/3qbOB2r) certain perpetrators of ransomware attacks and associated digital currency addresses as SDNs, including the Lazarus Group (https://bit.ly/3IPmzC0), Evil Corp (https://bit.ly/3GDZLn1), and the developer (https://bit.ly/31MI8Tq) of the Cryptolocker ransomware, heightening the risk that future ransomware payments may be demanded by an SDN, or an actor with ties to an SDN.

In addition, several major ransomware attacks in recent years involved a nexus to comprehensively sanctioned countries. For example, OFAC determined that certain Iranian persons were tied to the SamSam ransomware attacks starting in 2015. OFAC also found that the Lazarus Group, which developed the WannaCry 2.0 ransomware attack, was sponsored by North Korea.

Notably, any assessment of whether a ransomware attack has a sanctions nexus is complicated by difficulties in tracing the geographic origin of an attack and whether the attackers are affiliated with any sanctioned group, as well as the trend of well-known groups effectively "licensing" their software to unknown bad actors on the black market.

Cybersecurity policies and procedures are vital to preventing ransomware attacks in the first instance. Additionally, they may help reduce legal risk.

While the nexus to a sanctioned person or country may not be evident at the time a ransomware attack occurs, companies should consider whether to promptly report such attacks to law enforcement in order to claim voluntary disclosure credit from OFAC, and potentially disclose to OFAC itself.

Ransomware attacks also can expose companies to export controls-related risks. Specifically, when seizing control of an entity's systems and data, perpetrators may gain unauthorized access to technical data that is controlled for export under the International Traffic in Arms Regulations ("ITAR") or the Export Administration Regulations ("EAR").

Under these regulations, which are strict liability regimes, exfiltration of sensitive technical data to an unauthorized

destination or person could result in an export controls violation. The risk is especially pronounced under the ITAR, which imposes rigorous export licensing requirements for nearly all cross-border transfers of ITAR-controlled technical data.

Mitigating sanctions and export controls compliance risks

In the ransomware context, an overarching issue for a company to consider is cooperation with the authorities. Notably, the Advisory states that OFAC is more likely to resolve a sanctions violation with no enforcement action if a company reports to and cooperates with relevant authorities, including law enforcement, the Cybersecurity and Infrastructure Security Agency, and the Treasury Department's Office of Cybersecurity and Critical Infrastructure Protection. Crucially, OFAC noted that it will consider disclosure to such agencies, *"as soon as possible after discovery of an attack,"* to be a *"voluntary self-disclosure and a significant mitigating factor in determining an appropriate enforcement response."*

Companies should develop a base plan in advance of a ransomware attack to help companies quickly, thoughtfully, and comprehensively respond to such an attack and to help minimize legal risk.

This voluntary self-disclosure credit could result in a 50% reduction of potential OFAC penalties and other favorable treatment from OFAC. Governmental authorities may also have additional information about the perpetrator, including whether there is a sanctions nexus, which can help inform a company's response.

Furthermore, entities can take certain other steps both before a ransomware attack occurs and during the course of responding to an attack in order to mitigate sanctions and export controls risks.

1. Establish strong, risk-adjusted cybersecurity policies and procedures

Cybersecurity policies and procedures are vital to preventing ransomware attacks in the first instance. Additionally, they may help reduce legal risk. Notably, OFAC explicitly stated in the Advisory that it considers such policies and procedures to be a mitigating factor when determining whether to take enforcement action for sanctions violations arising from a ransomware attack.

2. Develop a plan in advance

Companies should develop a base plan in advance of a ransomware attack to help companies quickly, thoughtfully, and comprehensively respond to such an attack and to help minimize legal risk. Developing such a plan in advance helps a company to anticipate key issues and minimize potential risks in the fast-moving environment of an ongoing ransomware attack.

3. Work with cybersecurity and sanctions counsel

In addition to benefitting from the expertise of governmental authorities, companies can benefit from engaging cybersecurity and sanctions counsel early in the process. These experts can provide insight into how sanctions or export controls may be implicated by a company's particular circumstances and can assist in communicating with the relevant regulatory authorities.

Notably, the OFAC Advisory makes clear that both the company targeted by the attack and such experts should be mindful of the risks of facilitating ransom payments with a sanctions nexus.

4. Quickly secure any export-controlled technical data

Before a ransomware attack, companies should consider developing a mechanism to cut off all access to export-controlled technical data if a ransomware attacker breaches their systems or data.

Additionally, during an attack, companies should account for the technical data that an attacker could have accessed, so that such information can be shared with the Department of Commerce's Bureau of Industry and Security ("BIS") or the State Department's Directorate of Defense Trade Controls ("DDTC") in the event of a voluntary self-disclosure.

5. Identify any sanctions nexus

Though in many instances the identity of the perpetrator is unknown, companies may learn information about the perpetrator that helps to determine if there is a sanctions nexus. For example, IP logs may show that the perpetrator is from a particular sanctioned country. In addition, governmental authorities may have information about the perpetrator's identity that a company can compare against the SDN List to identify possible sanctioned persons.

On the other hand, however, there are certain challenges in identifying whether a perpetrator is based in a sanctioned country or affiliated with a sanctioned party, as perpetrators can launch attacks from countries in which they are not located and can conceal their identities. In any event, to the extent a company identifies a sanctions nexus, it should exercise heightened caution prior to making any ransom payments.

6. Maintain appropriate documentation

Through every step of the response to a ransomware attack, a company should maintain appropriate records of the remedial measures taken, communications with regulatory authorities, analyses regarding sanctions and export controls, and, if relevant, payments made. To the extent the company makes a voluntary self-disclosure or must answer questions from the authorities, such documentation is critical to demonstrating that a company followed best practices, such as those outlined in the Advisory.

7. Consider a voluntary self-disclosure

If a company identifies actual or potential violations of sanctions or export controls that arise from a ransomware attack, a voluntary self-disclosure to OFAC, BIS, and/or DDTC could be warranted.

Voluntary self-disclosures can help mitigate the likelihood of penalties or other public enforcement action related to violations, including by reducing applicable penalties by 50% and otherwise giving the company the opportunity to advocate to the regulator for leniency. Whether or not to disclose depends on the likelihood a violation occurred, the scope of potential violative conduct, and other case-by-case analysis.

About the authors



Anthony Rapa (L), a partner in **Kirkland & Ellis LLP**'s Washington, D.C., office, counsels companies and private equity sponsors regarding economic sanctions and export control issues in the context of corporate transactions and internal investigations. He can be reached at anthony.rapa@kirkland.com. **Carrie Schroll** (C) is a partner in the International Trade and National Security Practice Group in the firm's Washington, D.C., office, focusing her practice in the areas of export controls (ITAR and EAR), trade and economic sanctions (OFAC), customs, national security reviews by the Committee on Foreign Investment in the United States (CFIUS), anti-boycott restrictions, anti-money laundering (AML) regulations, and compliance with the U.S. Foreign Corrupt Practices Act (FCPA). She can be reached at carolyn.schroll@kirkland.com. **Sunil Shenoi** (R) is a partner in the Government & Internal Investigations Group in the Chicago office of the firm. He focuses his practice on advising clients on data security and data privacy matters, with a particular focus on responding to data breaches and defending against data breach litigation. He regularly advises clients on compliance with laws and regulatory guidance relating to data security and data privacy issues. He can be reached at sunil.shenoi@kirkland.com.

This article was first published on Reuters Legal News and Westlaw Today on December 16, 2021.