Improved Cybersecurity Can Mitigate Sanctions Risk and Other Takeaways from the Latest OFAC Advisory on Ransomware

September 23, 2021

On September 21, 2021, the U.S. Department of the Treasury's Office of Foreign Assets Control ("OFAC") issued an updated advisory (the "Advisory") on sanctions risks associated with payments to threat actors in connection with cyber ransoms. The Advisory reminds companies that all parties associated with the payment of a cyber ransom—including victims, financial institutions, insurance firms and other companies facilitating payment—are responsible for ensuring that they do not violate U.S. law and can be subject to an OFAC enforcement action if they do.

OFAC also named SUEX OTC, S.R.O. ("SUEX") as a malicious cyber actor, making SUEX the first virtual currency exchange to be designated as a sanctioned entity. According to OFAC and other industry intelligence, approximately 40% of SUEX's transactions involve illicit actors including nearly $13 million in transactions associated with ransomware operators since 2018.

Increased Risks of Inadvertent OFAC Violations. The Advisory largely tracks prior guidance, which we discussed in October 2020. But since then, the risk of inadvertently paying ransom to a sanctioned entity has increased as (1) some sanctioned threat actors have disbanded and reappeared with new names and updated tools, and (2) many non-sanctioned threat actors have been using tools developed by sanctioned threat actors or are otherwise partnering with sanctioned entities in their attacks.

Cybersecurity Compliance Can Mitigate the Risk of OFAC Enforcement. In light of this increased risk, the most significant development in the Advisory is an explicit recognition that having had enhanced cybersecurity controls in place prior to an attack can serve as a mitigating factor in a post-attack OFAC enforcement action in the event that a company has inadvertently made a cyber ransom payment to a sanctioned threat actor.

The Advisory encourages companies to implement a risk-based compliance program and adopt steps to reduce the risk of ransomware, including by adopting or improving practices such as those highlighted in the Cybersecurity Infrastructure Security Agency's ("CISA") September 2020 Ransomware Guide, which OFAC will consider "a

significant mitigating factor in any OFAC enforcement response." The practices outlined in that Guide include:

- Maintaining offline, encrypted backups of data and regularly testing these backups;
- Conducting regular vulnerability scanning to identify and address vulnerabilities;
- Regularly patching and updating software;
- Ensuring proper configuration of devices, including that security features are enabled;
- Employing best practices for remote desktop protocol ("RDP"), disabling or blocking Server Message Block ("SMB") protocol, restricting PowerShell usage;
- Securing domain controllers and Active Directory;
- Using application directory allowlisting on all assets to ensure that only authorized software can run; blocking all unauthorized software;
- Employing multi-factor authentication where possible and applying the principle of least privilege to all systems;
- Implementing logical or physical network segmentation to separate various business units, IT resources and operational technology environments;
- Retaining and securing network device and local host logs;
- Implementing a cybersecurity user awareness and training program;
- Understanding and mitigating the risk posed by third parties or managed service providers; and
- Creating, maintaining and exercising a basic cyber incident response and communications plan.

Diligence and Cooperation with Law Enforcement Are Additional Mitigation Factors. The Advisory provides that additional mitigation factors include (1) accounting for the risk that a ransomware payment may involve a sanctioned entity, (2) reporting the attack to the appropriate U.S. government agencies and (3) cooperating with those agencies. In particular, the Advisory provides that full and ongoing cooperation with law enforcement, both during and after a ransomware attack (e.g., providing all relevant information such as technical details, the ransom payment

demand and ransom payment instructions as soon as possible), will be a significant mitigation factor and will make it more likely that OFAC will resolve apparent violations with a nonpublic response (i.e., a No Action Letter or a Cautionary Letter). The Advisory also notes that OFAC will consider a company's self-initiated, complete and immediate report of a ransomware attack to law enforcement or other relevant U.S. agencies to be a voluntary self-disclosure, which is significant as voluntary self-disclosures are entitled to a 50% reduction on any potential penalty.

Presumption against Licenses. The Advisory also confirms prior OFAC guidance that because ransomware payments benefit illicit actors and undermine national security, there is a presumption of denial for license applications in this area.

Takeaways. In light of the Advisory, companies should consider the following steps to prepare for ransomware attacks and limit potential OFAC enforcement actions for inadvertent payments to sanctioned entities:

- **Sanctions and Cybersecurity Compliance Programs**. As we have advised previously, OFAC has made clear—independent of ransomware concerns—the importance of sanctions compliance programs and has highlighted five essential components: (1) management commitment, (2) risk assessment, (3) internal controls, (4) testing and auditing and (5) training. According to OFAC's Enforcement Guidelines, "the existence, nature, and adequacy" of such a program are factors that OFAC may consider when determining an appropriate enforcement action in the event of an apparent violation. Having a very strong cybersecurity compliance program, as outlined in the CISA Ransomware Guide (including testing incident response plans), is now another significant mitigation factor.

- **Prioritize Attribution**. As discussed above, identifying the threat actor in a ransomware investigation has become increasingly more difficult. Enhanced forensic tools and increased logging and detection can help companies more quickly identify and analyze ransomware variants and other indicators of compromise, which can be shared with law enforcement and experts to quickly identify the threat actor. The more certainty a company can achieve as to the identity of the attacker, the more confidence it can have in the sanctions risk associated with any payment.

- **Consider External Parties' Requirements**. OFAC's advisory is a reminder that the victim company is not the only entity associated with a ransom payment that can run afoul of U.S. sanctions laws. Insurance companies, financial institutions and ransom negotiators, among others, also carry this risk. It is therefore important that these entities receive prompt notice of the potential for payment so that their diligence processes do not cause unnecessary delays in a victim entity's negotiation strategy. Consequently, companies should consider identifying, as part of their

incident response planning, all the notifications and sanctions diligence that will be necessary before a payment can be made.

- **Transparency with Law Enforcement.** The FBI and other law enforcement agencies may be able to provide critical insight about an attack, including which threat group is associated with certain indicators or artifacts, and whether that group is associated with a sanctioned person or entity. OFAC has repeatedly emphasized the importance of promptly reporting ransomware incidents to law enforcement and providing ongoing cooperation throughout the investigation, and this Advisory again notes that prompt and complete reporting to law enforcement will be considered a voluntary self-disclosure. Companies should therefore consider having the contact information for key law enforcement agencies—including CISA and the local FBI field office—in their incident response plans and consulting with law enforcement before any payment is made.

We will closely follow developments in this area and provide any updates at the Debevoise Data Blog.

* * *

To subscribe to our Data Blog, please click here.

WASHINGTON, DC

Luke Dembosky
ldembosky@debevoise.com

Satish M. Kini
smkini@debevoise.com

NEW YORK

Avi Gesser
agesser@debevoise.com

SAN FRANCISCO

Sarah Quirk Smith
sqsmith@debevoise.com

H Jacqueline Brehmer
hjbrehmer@debevoise.com