OFAC and FinCEN Update Ransomware Guidance to Include New Red-Flag Indicators and Additional Sanctions Designations

November 10, 2021

On November 8, 2021, the U.S. Department of the Treasury ("Treasury") announced a new set of sanctions against criminal ransomware actors, the virtual currency exchange Chatex and three companies providing material support and assistance to Chatex. By designating these entities, which have direct ties with the previously sanctioned SUEX OTC, S.R.O. ("SUEX"), Treasury is suggesting that it will continue to use all tools available to identify and take action against those involved in facilitating ransomware payments.

Treasury's announcement also included an update to the Financial Crimes Enforcement Network ("FinCEN") 2020 Advisory on Ransomware and the Use of the Financial System to Facilitate Ransom Payments ("the Advisory"), which incorporates information recently released by FinCEN in its Financial Trend Analysis Report, including ransomware trends and typologies, associated payments and examples of recent ransomware incidents. While we recently discussed steps that financial institutions can take to mitigate sanctions risk associated with ransomware, the updated Advisory adds two new financial red-flag indicators for financial institutions:

1. Transfers involving a mixing service. Mixing services, or mixers, are websites or software designed to conceal the source or owner of a virtual currency. FinCEN's 2021 analysis indicates that mixers are commonly used by the top 10 ransomware variants.

2. Encrypted communications or portals. Communications with ransom recipients are often conducted through encrypted networks, such as TOR, or an unidentified web portal.

The combination of the updated Advisory and the new sanctions is a good reminder to companies of the increasing complexities surrounding ransomware payments. As more parties within the transaction lifecycle are designated as sanctioned entities and ransomware operators continue to share code and work together, the risk of inadvertently running afoul of sanctions laws will only increase.

With this in mind, companies should consider the following key takeaways to mitigating both their cybersecurity and legal risk:

1. Sanctions and Cybersecurity Compliance Programs. As we have previously discussed, OFAC has highlighted five essential components: (1) management commitment; (2) risk assessment; (3) internal controls; (4) testing and auditing; and (5) training. In its prior advisory, OFAC also suggested that a strong cybersecurity program, including as outlined in CISA's Ransomware Guide, is another significant mitigation factor. Adopting such a program will likely not only reduce the risk of a sanctions enforcement action but also minimize the likelihood of a ransomware event occurring.

2. Prioritize Attribution. While identifying the threat actor in a ransomware investigation has become more difficult, 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 payments. Diligence is especially critical given that attackers tend to work in groups using software-as-a-service structures, making it harder to identify whether the attacker is a sanctioned entity or affiliated with a sanctioned entity.

3. Consider External Parties' Requirements. Insurance companies, financial institutions, and ransom negotiators, among others, also carry the risk of violating U.S. sanctions laws. 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.

4. 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.

The authors would like to thank Debevoise law clerk Andreas Pavlou for his contribution to this article.

* * *

Please do not hesitate to contact us with any questions.

NEW YORK

Avi Gesser
agesser@debevoise.com

Aseel Rabie
arabie@debevoise.com

WASHINGTON, D.C.

Luke Dembosky
ldembosky@debevoise.com

Satish M. Kini
smkini@debevoise.com

SAN FRANCISCO

H Jacqueline Brehmer
hjbrehmer@debevoise.com