Client Alert

October 2020

Beware of Ransomware – Potential Sanctions Risk in Ransomware Payments

What Happened: The US warns victims of ransomware and companies facilitating ransomware payments of potential Office of Foreign Assets Control ("OFAC") violations in light of rising ransomware attacks.

The Bottom Line: Individuals and companies risk potential civil penalties based on strict liability if a ransomware payment involves a person or entity on OFAC's Specially Designated Nationals and Blocked Persons List ("SDN List").

The Full Story: The US Department of the Treasury's OFAC issued an advisory to cyberattack victims, financial institutions, cyber insurance firms, and other companies assisting with ransomware payments of potential civil penalties. The International Emergency Economic Powers Act ("IEEPA") and the Trading with the Enemy Act ("TWFA") generally prohibits individuals and companies under US jurisdiction from engaging in direct or indirect transactions with individuals and entities on the SDN List, other blocked persons, and those covered by country or region embargoes. Even non-US persons engaged in transactions that cause a person subject to US jurisdiction to violate IEEPA sanctions are at risk of violating these laws. Additionally, companies assisting in ransomware payments may have additional regulatory obligations under the Financial Crimes Enforcement Network ("FinCEN") regulations.

In a ransomware attack, cyber actors extort ransom payments from victims by blocking them from accessing their computer systems and data, typically with encryption, and then requesting payment to decrypt the information and return access. These cyber actors can cause millions of dollars in damages to US and international companies and their clients. Further, payment provides no guarantee cyber actors will return or protect the implicated information. Not to mention, these cyber actors often use ransom payments to undermine and fund activities adverse to US national security and foreign policy objectives.

OFAC applies a strict liability standard when imposing civil penalties for sanctions violations. Therefore, a US person may be civilly liable despite not knowing or having reason to know that they engaged in a transaction involving a person or entity included in OFAC's SDN List or covered by US embargoes. While companies can apply for a license to engage in these transactions, OFAC considers applications for ransomware payments with a presumption of denial.

Therefore, financial institutions and other companies assisting cyberattack victims are encouraged to develop risk-based compliance programs to mitigate their risk of violating US sanctions regulations. Additionally, the existence, nature and competence of these compliance programs are a mitigating factor OFAC considers when determining sanctions for possible violations. Significant mitigating factors include a company's timely and complete reporting of a cyberattack and its cooperation with law enforcement during and after the attack. Companies should review OFAC's Economic Sanctions Enforcement Guidelines for additional information on factors considered by OFAC for potential violations.

Individuals and companies subject to US jurisdiction and engaging in transactions involving ransomware payments should be aware of US sanctions regulations that may expose them to civil liabilities.

Hunton Andrews Kurth LLP will continue to closely monitor related developments on this issue and the broader US sanctions regime. Please contact us if you have any questions or would like further information regarding ransomware attacks.