DATA PRIVACY ALERT

NEAL GERBER EISENBERG

Potential Sanctions Risks for Facilitating Ransomware Payments

By: David A. Wheeler and Abigail Flores

October 7, 2020

On October 1, 2020, the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) issued an advisory to highlight the sanctions risks associated with ransomware payments related to malicious cyber-enabled activities. During the COVID-19 pandemic, demands for ransomware payments have increased as cyber actors target essential online systems. Companies that facilitate ransomware payments on behalf of victims, including financial institutions, cyber insurance firms, and companies involved in digital forensics and incident response may risk violating OFAC regulations.

Background on Ransomware Attacks

Ransomware is malicious software which blocks access to a computer system or data, often by encrypting data or programs on information technology systems. Such attacks frequently include threats to disclose victims' sensitive files. The cyber actors then demand a ransomware payment, usually through digital currency, in exchange for an encryption key to restore victims' access to systems or data.

OFAC Designations of Malicious Cyber Actors

OFAC has designated numerous malicious cyber actors under its cyber-related sanctions program and other sanctions programs, including perpetrators of ransomware attacks and those who facilitate ransomware transactions. Some cyber actors are listed on the Specially Designated Nationals and Blocked Persons List (SDN List), including the developers of Cryptolocker, SamSam, WannaCry 2.0, the Lazarus Group (a cybercriminal organization sponsored by North Korea), and Evil Corp (a Russia-based cybercriminal organization responsible for causing more than $100 million ransomware demands). OFAC has imposed, and will continue to impose, sanctions on these actors and others who materially assist, sponsor, or provide financial, material, or technological support for these activities.

Ransomware Payments with a Sanctions Nexus Threaten U.S. National Security Interests

Facilitating a ransomware payment that is demanded as a result of malicious cyber activities may enable criminals and adversaries with a sanctions nexus to profit and advance their illicit aims. Payments made to sanctioned persons or jurisdictions could be used to fund activities adverse to the national security and foreign policy objectives of the United States. Ransomware payments may also embolden cyber actors to engage in future attacks. In addition, paying a ransom does not guarantee that the victim will regain access to its stolen data.

Facilitating Ransomware Payments on Behalf of a Victim May Violate OFAC Regulations

Under the authority of the International Emergency Economic Powers Act (IEEPA) or the Trading with the Enemy Act (TWEA),[1] U.S. persons are generally prohibited from engaging in transactions, directly or indirectly, with individuals or entities on OFAC's SDN List, other blocked persons, and those covered by comprehensive country or region embargoes (e.g., Cuba, the Crimea region of Ukraine, Iran, North Korea, and Syria). Additionally, any transaction that

1 50 U.S.C. §§ 4301–41; 50 U.S.C. §§ 1701–06.

causes a violation under IEEPA, is also prohibited. OFAC may impose civil penalties for sanctions violations based on strict liability, meaning that a person subject to U.S. jurisdiction may be held civilly liable even if they did not know or have reason to know they were engaging in a transaction with a person that is prohibited under sanctions laws and regulations administered by OFAC. Further, companies involved in facilitating ransomware payments on behalf of victims should also consider whether they have regulatory obligations under Financial Crimes Enforcement Network (FinCEN) regulations.

Under OFAC's Enforcement Guidelines, OFAC will also consider a company's self-initiated, timely, and complete report of a ransomware attack to law enforcement to be a significant mitigating factor in determining an appropriate enforcement outcome if the situation is later determined to have a sanctions nexus. It may also consider the existence, nature, and adequacy of a sanctions compliance program when determining an appropriate enforcement response for a violation of a sanctions laws or regulations. OFAC will also consider a company's full and timely cooperation with law enforcement both during and after a ransomware attack to be a significant mitigating factor when evaluating a possible enforcement outcome.

Based on the risks associated with paying ransomware demands and potential OFAC civil penalties, companies should review legal and regulatory obligations in connection with cybersecurity contingency and disaster recovery planning.

This alert was authored by

David A. Wheeler | 312-269-5328 | dwheeler@nge.com
Abigail Flores | 312-269-1739 | aflores@nge.com

If you have any questions regarding review of cybersecurity measures or the OFAC advisory, please contact David Wheeler, Abigail Flores or your Neal Gerber Eisenberg attorney.
