BRACEWELL

INSIGHTS

Ransomware Victims Told to Think Twice Before Paying Hackers

September 22, 2021

By: ***Seth D. DuCharme***

On Tuesday, the U.S. Department of Treasury's Office of Foreign Asset Control ("OFAC") issued an ***updated advisory*** warning all ransomware victims that if they succumb to ransomware demands and pay foreign actors who are subject to U.S. sanctions, the victims could face further financial peril. OFAC articulated that imposing sanctions is an appropriate step, aimed at disrupting the economic infrastructure of the ransomware threat that has surged over the last year and targeted countless corporations and critical infrastructure. While the advisory does not change existing law, it signals increased regulatory enforcement and an intent to put companies on notice that they will have an even more complicated risk analysis to conduct when faced with a ransomware attack. It also underscores the importance of having an updated incident response plan, as well as the need for victims of ransomware attacks to have the correct incident response team in place, prior to any attack, to ensure compliance with the law when responding to an attack of this nature.

Reiterating the federal government's strong discouragement against paying ransom after a cyber-attack, the latest OFAC advisory also alerts organizations of the steep civil penalties that may come with making ransom payments to a person or group on the Specially Designated Nationals and Blocked Persons List ("SDN List"). According to the guidance, OFAC may impose civil penalties of up to $20 million for sanctions violations based on strict liability, meaning that the victim company may be held civilly liable even if they did not know they were engaging in a transaction that was prohibited under sanctions laws.

Additionally, in a significant change from previous guidance, OFAC now "strongly encourages" all victims of ransomware attacks to report the incidents to CISA and FBI, or the U.S. Secret Service. In doing so, victim companies can receive significant mitigation from OFAC when determining an appropriate enforcement response. While not creating a mandatory ransomware notification rule, OFAC's latest advisory creates a strong incentive for companies involved in a ransomware attack to notify law enforcement, even when where there is no known sanctions nexus, to take advantage of the enforcement mitigation in the event of an inadvertent violation.

The OFAC advisory also notes that adopting and improving cybersecurity practices will be considered a significant mitigating factor for enforcement purposes. In addition to developing incident response plans, such steps could include maintaining offline backups of data, instituting cybersecurity training, regularly updating antivirus and anti-malware software, and employing authentication protocols, among others. CISA has recently released a "***Cyber***

Security Evaluation Tool" to assess varying levels of ransomware threat readiness to be helpful to all organizations regardless of their cybersecurity maturity.

While it is not new that the U.S. government strongly discourages ransomware payments, the latest advisory made one major point clear: OFAC is focused on disrupting criminals' ability to anonymously profit from attacks, and it is willing to at least threaten greater punishments on victims who do not notify law enforcement and who elect to pay ransomware attackers. This recent guidance from OFAC creates even more incentives for private sector companies to implement robust compliance and cybersecurity programs in place to account for the need to identify hackers, and to work closely with federal law enforcement to mitigate the consequences that can flow from a ransomware attack. If you have any questions about how any of these issues might impact your business, our attorneys are ready to help.