akerman

Practice Update

New OFAC Advisory Offers Steps to Reduce Sanctions Risks for Entities Facilitating Ransomware Payments

September 24, 2021

By Elizabeth F. Hodge and Christy S. Hawkins

Companies that make ransomware payments, whether they be the victim of a ransomware attack or entities that facilitate such payments, should review the updated advisory issued by U.S. Department of the Treasury's Office of Foreign Asset Control (OFAC) to understand the sanctions risk associated with ransomware payments and, importantly, proactive steps they can take to mitigate those risks. Specifically, OFAC elaborates on its prior guidance regarding reporting and cooperation by companies and addresses defensive measures to reduce the risk of becoming a victim of a ransomware attack.

The September 21, 2021 Updated Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments (the "Updated Advisory") follows the initial October 2020 OFAC advisory (the "October 2020 Advisory") that generated concern among those businesses that might facilitate ransom payments and those businesses who feared being the victim of a ransomware attack. The October 2020 Advisory put such companies on notice that facilitating ransomware payments, either on their own behalf or on behalf of a victim, may violate OFAC regulations and subject them to strict liability for civil penalties. In the Updated Advisory, OFAC expands on the discussion of potential mitigating

Related People

Christy S. Hawkins
Elizabeth F. Hodge

Related Work

Data Privacy and Security

factors identified in the October 2020 Advisory and says that it will consider the following factors when assessing appropriate enforcement for an apparent violation of U.S. sanctions laws:

1. Implementing a risk-based compliance program to minimize the risk that a ransomware payment may involve a Specially Designated National (SDN) or blocked person. OFAC previously explained that financial institutions, providers of cyber insurance, digital forensics and incident response vendors, and money services businesses should adopt a compliance program to reduce the risk that they will conduct a transaction with a sanctions nexus.
2. Reducing the risk of a ransomware attack by implementing robust cybersecurity practices. OFAC reiterates that it strongly discourages "all private companies and citizens" from paying ransom or extortion demands. Instead, businesses should focus on strengthening their defensive and resilience measures to prevent ransomware attacks in the first place by adopting or improving cybersecurity practices, such as those highlighted in the Cybersecurity and Infrastructure Security Agency's (CISA) September 2020 Ransomware Guide, "will be considered a significant mitigating factor in any OFAC enforcement response." Some meaningful steps OFAC identifies include:
    - maintaining offline backups of data,
    - developing and testing incident response plans,
    - cybersecurity training,
    - regularly updating antivirus and anti-malware software, and
    - employing authentication protocols.
3. Timely reporting of ransomware attacks to appropriate U.S. government agencies and the extent and nature of cooperation with OFAC and other government agencies. The Updated

- Advisory expands on OFAC's prior statements that it will consider a company's prompt reporting of a ransomware attack to appropriate law enforcement agencies and the nature and extent of cooperation with OFAC, law enforcement, and other relevant government agencies to be a mitigating factor. Where a ransomware payment may have a sanctions nexus, OFAC says it will consider a company's "self-initiated and complete" report of a ransomware attack to law enforcement made "as soon as possible after discovery of the attack" to be a voluntary self-disclosure and a significant mitigating factor.

OFAC also reiterates its position in the October 2020 Advisory that it will continue to review license applications involving ransomware payments demanded as a result of malicious cyber activities on a case-by-case basis with a presumption of denial.

Given the frequency of ransomware attacks and OFAC's continuing emphasis on preventing ransomware payments to sanctioned entities, companies should review the Updated Advisory and consider what steps they will take to minimize their risk of civil penalties due to ransomware payments with a sanctions nexus.
