Armstrong Teasdale

September 30, 2021 • Advisory • www.atllp.com

AS CYBERSECURITY INCIDENTS INCREASE, OFAC REVISES POLICY ON RANSOMWARE

It's no secret that the frequency and impact of cybersecurity incidents involving ransomware have increased dramatically. In 2020, the Institute for Security + Technology reported that nearly 2,400 U.S.-based governments, health care facilities and schools were victims of ransomware. The average ransomware payment rose 171% to $312,493. In a 2020 survey of 5,000 IT managers, 51% indicated that they had been attacked by ransomware in the last year.

In response, the Department of the Treasury's Office of Foreign Assets Control (OFAC) recently issued an advisory which revises their policy on potential sanctions risks for companies that make ransomware payments. In doing so, OFAC emphasizes that the U.S. government strongly discourages all private companies and citizens from paying ransom or extortion demands, and instead recommends focusing on strengthening defensive and resilience measures to protect against these attacks.

THE POLICY AND IMPACT ON COMPANIES

The policy prohibits any transactions, directly or indirectly, made to malicious cyber actors who have been designated under OFAC's cyber-related sanctions program. The advisory indicates that these transactions are prohibited since ransomware payments may allow those who have been sanctioned to "profit and advance their illicit aims." OFAC further reasons that "such payments not only encourage and enrich malicious actors, but also perpetuate and incentivize additional attacks."

The policy empowers OFAC to impose civil penalties for sanctions violations based on strict liability—meaning that a person may be held civilly liable even if the person did not know or have reason to know that the action was prohibited. These enforcement actions can take several different forms, ranging from non-public responses such as a No Action Letter or a Cautionary Letter, to public responses such as civil monetary penalties.

HOW TO AVOID A CIVIL PENALTY

The advisory contains several mitigating factors that OFAC may consider when determining an appropriate enforcement response to an alleged violation. OFAC highlights the importance of compliance programs and cooperation with

PEOPLE

F. Scott Galt, CIPP/E

SERVICES AND INDUSTRIES

Data Innovation, Security and Privacy

International

Governance and Compliance

law enforcement. While the resolution of each potential enforcement is fact-specific, OFAC is more likely to resolve violations involving ransomware attacks with a non-public response when the victim takes the mitigating steps that include:

- a Sanctions Compliance Program (SCP);
- meaningful steps to improve cybersecurity practices, such as those highlighted in CISA's Ransomware Guide which include:
    - An Incident Response Plan (IRP)
    - A Written Information Security Program (WISP)
    - Maintaining offline backups of data
    - Instituting cybersecurity training
    - Regularly updating antivirus and anti-malware software
    - Employing authentication protocols
- making a voluntary and complete self-disclosure report of the ransomware attack to OFAC, law enforcement, or other appropriate U.S. agencies; and
- the company's cooperation with OFAC/law enforcement.

The above mitigating factors are merely starting points that are considered by OFAC when determining an appropriate enforcement response in the event a sanctions nexus is found in connection with a ransomware payment.

Armstrong Teasdale's Privacy and Data Security attorneys have significant experience guiding clients in developing and maintaining SCPs, IRPs and WISPs. We also have significant experience building and auditing risk-based compliance programs to mitigate exposure to sanctions- and embargoes-related violations. We will continue to monitor and provide updates regarding OFAC and other cybersecurity developments. Please contact your regular AT attorney or one of the authors listed below for proactive guidance specific to your business.