STEPTOE OUTSIDE COUNSEL

# Ransomware – is your compliance program ready?

Every company dreads becoming the victim of a ransomware attack. Well-prepared companies will have a plan and spring into action. OFAC's recent guidance has underscored why compliance personnel for companies – and their insurers, financial institutions, and other "facilitators" – need to ensure that sanctions compliance is adequately integrated into their ransomware action plans.

Last month, the Office of Foreign Assets Control ("OFAC") updated its prior (2020) advisory highlighting sanctions risks for making or facilitating ransomware payments. The advisory follows several high-profile ransomware attacks, including a number in sensitive industries, resulting in increased US government attention.

OFAC "strongly discourages" victims from making ransom payments. At the same time, the advisory sets out ways that victims and other parties involved in facilitating payments, can reduce the likelihood of enforcement in the event a ransomware payment involves a sanctioned person or jurisdiction. Here are the key takeaways:

- **Invest in cybersecurity.** According to OFAC, "meaningful steps taken to reduce the risk of extortion by a sanctioned actor through adopting or improving cybersecurity practices" will be considered a "significant mitigating factor" under OFAC's enforcement guidelines. What does this mean? OFAC suggests steps like "maintaining offline backups of data, developing incident response plans, instituting cybersecurity training, regularly updating antivirus and anti-malware software, and employing authentication protocols, among others."

- **Report ransomware attacks… quickly.** OFAC says it "will consider a company's self-initiated and complete report of a ransomware attack to law enforcement or other relevant agencies … made as soon as possible after the discovery of an attack, to be a voluntary self-disclosure and a significant mitigating factor" in any enforcement action. OFAC will also consider ongoing cooperation with law enforcement during and after a ransomware attack to be mitigating. This means, for example, "providing all relevant information such as technical details, ransom payment demand, and ransom payment instructions as soon as possible." This is notable because OFAC does not typically treat disclosure to another government agency as a voluntary self-disclosure to OFAC. This language appears intended to balance OFAC's interest in victims' timely reporting of ransomware attacks with the fast moving nature of such attacks and victims' responses. The updated guidance adds, "OFAC would be more likely to resolve apparent violations involving ransomware attacks with a non-public response (i.e., a No Action Letter or a Cautionary Letter) when the affected party" took "mitigating steps… particularly reporting the ransomware attack to law enforcement as soon as possible and providing ongoing cooperation."

- **Cooperate with regulators.** OFAC will consider the "nature and extent" of a victim's cooperation with OFAC, law enforcement, and other relevant agencies in determining how to enforce apparent sanctions violations in a ransomware context.

- **Revisit your compliance program.** OFAC's revised guidance continues to emphasize the importance of addressing ransomware risks as part of a comprehensive sanctions compliance program. In particular, entities engaged in cyber insurance, digital forensics and incident response, and financial services, that may assist victims in responding to attacks and making ransom payments, should "account for the risk that a ransomware payment may involve an SDN or blocked person, or a comprehensively embargoed jurisdiction" as part of their larger sanctions compliance programs.

Compliance officers would be well advised to review their current compliance programs and, if warranted, make appropriate updates in light of OFAC's revised advisory.

Observant compliance officers can play a key role in reducing the risk of a sanctions violation in the event of a ransomware attack, and can position a company to mitigate its enforcement risks if an attack occurs. ■

About the authors:

Meredith Rathbone is a Partner and Evan Abrams is an Associate in the Washington, DC office of Steptoe. www.steptoe.com

Reprinted with permission from the October 2021 issue of Export Compliance Manager.
www.exportcompliancemanager.com