KAUFMAN | DOLOWICH

Mansfield Rule Certified 2022-2023

New Ransomware Advisory Warns of Penalties for Ransom Payments

By Henry Norwood, Attorney

The fight against the scourge of the data privacy world, ransomware, has taken a new turn as the U.S. federal government has issued new guidance making clear that victims of ransomware attacks who opt to pay ransom demands may in turn face government-imposed penalties.

On October 1st, 2020, in the face of rising ransomware attacks throughout the Covid-19 pandemic, the U.S. Department of Treasury published its Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments.[i] The Advisory notes that institutions often involved in facilitating payments to ransomware hackers, including cyber insurers, digital forensics firms, and financial institutions are part of the ransomware problem in that they encourage hackers to continue deploying the virus and that these institutions may actually be in violation of the Department of Treasury's Office of Foreign Assets Control (OFAC) sanctions regulations. Specifically, OFAC designates malicious actors under its cyber sanctions program and prohibits U.S. organizations from providing material support to these malicious actors. Several active cybercriminal organizations as well as the developers of certain, successful ransomware variants have been labeled as malicious actors by OFAC and thus financial payments to these actors are prohibited.

In the context of a ransomware attack, the victim of the attack, their insurer, a digital forensics organization hired to provide support, a financial institution, or any other entity (although not explicitly mentioned in the advisory, law firms who assist in these payments would also likely be subject to the same rules) involved in the attack response would be prohibited from making any form of payment to the hacker in exchange for the release and/or non-disclosure of the compromised data if the hacker has been designated a malicious actor under OFAC's cyber sanctions program. The clear issue that arises here is that determining the identity of a ransomware hacker is often beyond the ability of non-government organizations, particularly when these organizations are primarily concerned with protecting their compromised data and mitigating the harm of an ongoing ransomware attack. In deciding whether to make a ransom payment, cyber response teams will now need to weigh the possibility of penalties if they cannot ascertain the identity of their attacker.

The Department of Treasury Advisory provides guidance on the penalties that may be imposed on those who pay ransomware hackers as well. Importantly, the Advisory makes clear that entities may be held liable for payments to ransomware hackers even if they are unaware of a legal violation under a strict liability scheme. The Advisory also references a penalty schedule provided in 31 C.F.R. part 501, appx. A[ii] with the severity of the monetary penalty dependent on the amount paid to a ransomware hacker.

OFAC has discretion regarding whether, and to what extent, it will penalize entities making payments to ransomware hackers. The factors OFAC will weigh in determining the severity of a penalty for violating this prohibition are found in the Code of Federal Regulations[iii] and include: (1) whether the violation of OFAC's regulation was willful or reckless; (2) whether the at-fault party was aware of its own conduct; (3) the harm to the goals of OFAC's cyber sanctions program; (4) the characteristics specific to the at-fault party, including their size and commercial sophistication; (5) whether the party had a cyber compliance program in place; (6) the remedial actions taken by the party; and (7) the party's cooperation with OFAC throughout the investigative process.

The new Advisory represents the federal government's approach to curb ransom payments to hackers, but at the same time, the Advisory raises several additional hurdles for entities enduring a ransomware attack as well as the response teams in place to aid ransomware victims. Organizations maintaining private, valuable data should take a proactive approach by implementing cyber legal compliance programs in anticipation of a ransomware attack. Such programs should incorporate OFAC's seven-factor analysis to limit any potential liability to the federal government, while also promoting the organization's primary goal of protecting

[i] https://home.treasury.gov/system/files/126/ofac_ransomware_advisory_10012020_1.pdf

[ii] 31 C.F.R. part 501, appx. A.

[iii] Id.