Published on *The National Law Review* https://www.natlawreview.com

Update: Ransomware: To Pay or Not to Pay

Article By:

Linn F. Freedman

Three recent events are prompting me to update our previous blog post on the difficult decision of whether to pay or not to pay ransomware following an attack [view related post].

The first event is that the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) issued an advisory on October 1, 2020, "to highlight the sanctions risks associated with ransomware payments related to malicious cyber-enabled activities." The advisory warns that if a company or a vendor facilitates the payment of a ransom to criminals or adversaries "with a sanctions nexus," the funds could be used "to fund activities adverse to the national security and foreign policy objectives of the United States." Therefore, companies or vendors acting on their behalf who pay a ransom to a sanctioned individual or governments are at risk for sanctions under the Financial Crimes Enforcement Network (FinCEN) regulations.

The advisory is a very important consideration to weigh in determining whether or not to pay a ransom for encryption keys or destruction of data.

The second event was a recent thoughtful analysis on this subject matter by KrebsonSecurity, entitled "Why Paying to Delete Stolen Data is Bonkers." Referring to a Coveware report, which states that almost half of all ransomware cases include the release of exfiltrated data, Krebs quotes from the Report "Unlike negotiating for a decryption key, negotiating for the suppression of stolen data has no finite end."

Krebs further notes that ransomware victims who pay for the decryption key are relying on hope that the keys will work, which is not always the case.

The final event is that there is growing anecdotal evidence that Ransomware as a Service (RaaS) operators, usually less sophisticated than the big boys, are engaging in double extortion scams against their victims. This means that if you have made the business decision to pay the ransomware for either the decryption keys or the destruction of data, these operators are refusing, after you have agreed to pay a negotiated amount, and they have initially agreed to hold up their part of the bargain, to give you the key or the confirmation of destruction until you pay more ransom. This behavior is certainly inconsistent with the general business plan of ransomware that the attackers will return what has been ransomed after payment, so future victims can be assured that if they pay the ransom, they will get their keys or the data back. This new phenomenon provides a strong argument (in addition to

the ones above) to refrain from paying the ransom. They are criminals, after all, and some are more credible and smarter than others. These attackers who engage in double extortion will rapidly get a bad reputation and are shooting themselves in the foot. However, while in the midst of the attack, you just don’t know who you are dealing with, so weighing these risks is challenging at best.

National Law Review, Volumess X, Number 337