Companies Face Increased Sanctions Risk for Making Ransomware Payments—Takeaways from the Latest OFAC and FinCEN Advisories

October 7, 2020

Earlier this year, we shared a list of 13 technical and nontechnical measures companies can adopt to mitigate the risks of ransomware attacks. With ransomware and other malicious cyber-related attacks continuing to grow in frequency, scope and sophistication, two divisions within the U.S. Treasury Department issued advisories last week detailing risks and considerations regarding financial transactions related to these events. Specifically, on October 1, 2020, the Office of Foreign Assets Control ("OFAC") and the Financial Crimes Enforcement Network ("FinCEN") issued companion advisories on ransomware payment risks (the "OFAC Advisory" and "FinCEN Advisory," respectively).

The issuance of these twin advisories suggests heightened concern among regulatory and law enforcement authorities, including as to the involvement of incident response, forensics and cyber insurance companies in making ransomware payments. Although assessing the legality of ransom payments has always been a priority consideration for those on the frontlines of advising and assisting companies with cyber incident responses, the advisories serve as a helpful reminder of the various considerations, and serious consequences, involved.

The OFAC Advisory explains that a U.S. company victimized by ransomware attacks, as well as U.S.-based firms that facilitate negotiations with cybercriminals, may be held civilly liable for sanctions violations even if they are unaware that transactions may involve persons or entities subject to sanctions. That sanctions risks are associated with ransomware payments is not news; OFAC has for several years designated for sanctions both criminal perpetrators of ransomware attacks and those who "materially assist, sponsor, or provide financial, material, or technological support for these activities." Similarly, in July this year, the EU imposed asset freezes prohibiting payments to six individuals and three entities associated with the "WannaCry", "NotPetya", and "Operation Cloud Hopper" campaigns. It is noteworthy, however, that OFAC chose to emphasize in its advisory the availability of civil penalties on a strict-liability basis for sanctions violations by all parties involved in "digital forensics and incident response" that play a role in "facilitat[ing] ransomware payments."

The FinCEN Advisory describes red flags for financial institutions that may be indicative of "ransomware-related illicit activity." It also warns that incident response vendors and cyber insurers may be required to register as money services businesses if they facilitate ransomware payments. Such registration triggers record keeping and compliance obligations imposed under the Bank Secrecy Act, including the requirement to file suspicious activity reports.

Together, these advisories underscore the importance for companies to implement five key risk mitigation strategies to prepare for ransomware attacks:

1. **Maintain an open line of communication with law enforcement contacts** who may be able to provide insights about the ransomware group in question including whether the group may be associated with a sanctioned person or entity. This is especially critical not only in light of OFAC's strict liability-based civil penalty regime, but also because under OFAC's Enforcement Guidelines (and recited in the OFAC Advisory) "a company's self-initiated timely, and complete report of a ransomware attack to law enforcement" is considered a significant mitigating factor in OFAC's enforcement considerations;
2. **Retain seasoned outside experts**—forensic investigators and cyber counsels—who are familiar with responding to particular variants of ransomware attacks and who often have contacts in law enforcement that can help identify the attacker and evaluate the risks of negotiating or making a payment;
3. **Involve cyber insurers early in the incident response** especially as they now may have heightened expectations to be involved in the decision process regarding ransom payment;
4. **Develop a plan to guide key decision-makers in their evaluation of ransom payment** strategy as well as sanctions and other (*e.g.*, corporate governance, securities law) compliance considerations. Now might be a good time to see if your company's incident response plan could use a refresh. If it already has a ransomware module per guidance from the SEC earlier this year, consider whether it needs to be updated with the latest considerations on ransom payment; and
5. **Ensure your company has in place a risk-based sanctions compliance program** to mitigate exposures to sanctions-related violations. As we have advised previously, OFAC has made clear the importance of such programs. According to OFAC's Enforcement Guidelines, "the existence, nature, and adequacy" of such a program are factors that OFAC may consider when determining an appropriate enforcement action in the event of an apparent violation.

Whether to make a ransomware payment is always a difficult decision, and one that is often made with limited information and significant risks. Payment does not guarantee

delivery of the advertised decryption or deletion of the hostage data. And even if the attackers do keep their promises, payment puts money into the hands of criminal organizations who use the money to develop more sophisticated attacks against innocent businesses, even if those attacks do not rise to the level of directly threatening U.S. national security. In fact, all these factors recently led the French cybersecurity agency to issue guidance earlier this month encouraging companies not to pay ransoms. But, despite these apparent risks, companies often feel that they have no choice and must bargain with the devil to save their business.

We are not aware of a company that has been prosecuted for making ransom payments, presumably because these incidents have historically presented sound policy reasons and strong defenses against prosecution. The OFAC Advisory seems to acknowledge this—at least in a limited fashion—in reciting certain mitigation factors from its Enforcement Guidelines.

Nevertheless, the twin advisories from OFAC and FinCEN may signal increased regulatory oversight in this area and may foreshadow a more aggressive enforcement posture going forward. The same may also be true in the EU now that its first cyber-specific asset freezes are in place with more likely to follow in the future.

The OFAC and FinCEN guidance are likely to have two practical implications for organizations considering ransom demands. First, victims may be more reluctant to make a ransom payment if they cannot determine with whom they are dealing, for fear of being caught up in OFAC's strict liability regime. This, in turn, may result in more companies involving outside experts and law enforcement early in the process to help identify the attacker and confirm that they are not subject to OFAC sanctions. Second, companies may spend more time testing their backups, running tabletops and implementing other measures that will limit the damage a ransomware attack may cause, in case making a payment is not an option.

We will closely follow developments in this area and provide any updates at the Debevoise Data Blog.

* * *

Please do not hesitate to contact us with any questions.

To subscribe to our Data Blog, please click here.

The authors would like to thank Debevoise trainee associate Jesse Hope for his contribution to this article.

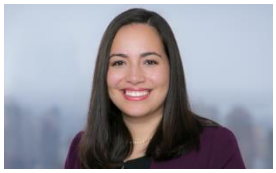
NEW YORK


Jeremy Feigelson
jfeigelson@debevoise.com


Avi Gesser
agesser@debevoise.com


Paul M. Rodel
pmrodel@debevoise.com

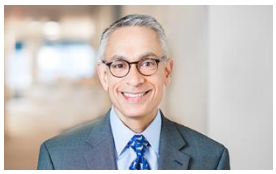

David G. Sewell
dsewell@debevoise.com


Zila Reyes Acosta-Grimes
zracostagrimes@debevoise.com


Mengyi Xu
mxu@debevoise.com

WASHINGTON, D.C.


Luke Dembosky
ldembosky@debevoise.com


Satish M. Kini
smkini@debevoise.com

LONDON


Martha Hirst
mhirst@debevoise.com


Robert Maddox
rmaddox@debevoise.com