King & Spalding
Client Alert

OCTOBER 12, 2020

Ransomware: To Pay or Not to Pay?

For more information, contact:

Scott Ferber
+1 202 626 8974
sferber@kslaw.com

Phyllis Sumner
+1 404 572 4799
psumner@kslaw.com

King & Spalding

Washington, D.C.
1700 Pennsylvania Avenue, NW
Washington, D.C. 20006-4707
Tel: +1 202 737 0500

Atlanta
1180 Peachtree Street, NE
Atlanta, Georgia 30309-3521
Tel: +1 404 572 4600

Ransomware has emerged as one of the most virulent cybersecurity risks, affecting public and private sector alike.[1] In recent years, ransomware attacks have become more focused, sophisticated, costly, and numerous. Threat actors have shifted their tactics and techniques to include the destabilizing combination of encryption, data exfiltration, and company-shaming to attempt to extract sizable payments from their victims. According to the FBI, there was a 37% annual increase in reported ransomware cases and a 147% annual increase in associated losses from 2018 to 2019.[2] The number of ransomware incidents continues to increase in 2020.[3] Ransom payment amounts also reportedly are on the rise. The average ransom payment in the second quarter of 2020 was $178,254 – a 60% jump from the previous quarter.[4] Seven-figure demands are not uncommon. Security experts say that even these numbers underestimate the true cost of ransomware attacks, which have disrupted factories and basic infrastructure and forced businesses to shut down.

Ransomware has been forging new ground in 2020, with cyber criminals using COVID-19 as another deployment lure.[5] This threat is not expected to go away anytime soon, with the FBI's anticipating that malign actors will exploit increased use of virtual environments as a result of the pandemic.[6]

What is an organization to do when faced with a ransomware attack?

On the threshold question of whether to pay, the FBI "advocate[s]" against it, in part because payment does not guarantee an organization will regain access to its data. The FBI nonetheless acknowledges "that when businesses are faced with an inability to function, executives will evaluate all options to protect their shareholders, employees, and customers."[7]

Ransomware victims and the white hat organizations with whom they work to address an attack (such as cyber insurance, digital forensics and incident response, and financial services that may involve processing ransom payments) also should be mindful of the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) recent advisory on potential sanctions risks associated with ransomware payments.[8]

Key takeaways from this advisory are:

- OFAC has designated "numerous" malicious cyber actors under its cyber-related sanctions program and other sanctions programs, including perpetrators of ransomware attacks and those who facilitate ransomware transactions.
- Under the authority of the International Emergency Economic Powers Act (IEEPA) and Trading with the Enemy Act (TWEA), U.S. persons generally are prohibited from engaging in transactions, directly or indirectly, with individuals or entities on OFAC's Specially Designated Nationals and Blocked Persons List (SDN List), other blocked persons, and those covered by comprehensive country or region embargoes.
- Any transaction that causes a violation under IEEPA, including transactions by a non-U.S. person which causes a U.S. person to violate any IEEPA-based sanctions, is prohibited.
- U.S. persons, wherever located, are generally prohibited from facilitating actions of non-U.S. persons, which could not be directly performed by U.S. persons due to U.S. sanctions regulations.
- OFAC can impose civil penalties for sanctions violations based on strict liability.
- OFAC encourages financial institutions and other companies – including those that engage with victims of ransomware attacks – to implement a risk-based compliance program to mitigate exposure to sanctions-related violations.
- OFAC will consider a company's "self-initiated, timely, and complete" report of a ransomware attack to law enforcement to be a "significant mitigating factor" in determining an appropriate enforcement outcome if the situation is later determined to have a sanctions nexus.
- OFAC also will consider a company's "full and timely cooperation" with law enforcement both during and after a ransomware attack to be a "significant mitigating factor" when evaluating a possible enforcement outcome.

There are no easy answers to the difficult question of whether to pay. Companies must balance potential near-term benefit of decrypting data, which is not always guaranteed, against the risk of legal exposure for making a payment to a prohibited person or entity – not to mention the risk of increased targeting by threat actors once a payment has been made. Waiting until right-of-boom to assess these issues only will complicate the situation. As OFAC's advisory makes clear, companies should have a plan in place before an attack ever occurs.

[1] Ransomware is a form of malware designed to block access to a computer system or data, often by encrypting data or programs on information technology systems to extort ransom payments from victims in exchange for decrypting the information and restoring victims' access to their systems or data. In some cases, in addition to the attack, malign actors threaten to publicly disclose victims' sensitive files that they have stolen from victims' systems. The malign actors then demand a ransomware payment, usually through digital currency, in exchange for a key to decrypt the files and restore victims' access to systems or data. FBI IC3 PSA, *High-Impact Ransomware Attacks Threaten U.S. Business and Organizations*, available at https://www.ic3.gov/media/2019/191002.aspx (Oct. 2, 2019).

[2] *See* FBI IC3, *2018 Internet Crime Report*, available at https://pdf.ic3.gov/2018_IC3Report.pdf; FBI IC3, *2019 Internet Crime Report*, available at https://pdf.ic3.gov/2019_IC3Report.pdf.

[3] *See* Verizon, 2020 Data Breach Investigations Report, available at https://enterprise.verizon.com/resources/reports/2020-data-breach-investigations-report.pdf.

[4] *See* Coveware, *Ransomware Attacks Fracture Between Enterprise and Ransomware-as-a-Service in Q2 as Demands Increase*, available at https://www.coveware.com/blog/q2-2020-ransomware-marketplace-report (Aug. 3, 2020).

[5] *See* FBI Press Release, *FBI and Secret Service Working Against COVID-19 Threats*, available at https://www.fbi.gov/news/pressrel/press-releases/fbi-and-secret-service-working-against-covid-19-threats (Apr. 15, 2020); FBI IC3 PSA, *FBI Sees Rise in Fraud Schemes Related to the COVID-19 Pandemic*, available at https://www.ic3.gov/media/2020/200320.aspx (Mar. 20, 2020).

[6] *See* FBI IC3 PSA, *Cyber Actors Take Advantage of COVID-19 Pandemic to Exploit Increased Use of Virtual Enviroments*, available at https://www.ic3.gov/media/2020/200401.aspx (Apr. 1, 2020).

[7] *See* FBI IC3 PSA, *High-Impact Ransomware Attacks Threaten U.S. Business and Organizations*, available at https://www.ic3.gov/media/2019/191002.aspx (Oct. 2, 2019).

[8] *See* U.S. Dep't of Treasury, *Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments*, available at https://home.treasury.gov/system/files/126/ofac_ransomware_advisory_10012020_1.pdf (Oct. 1, 2020).