Schulte Roth&Zabel
Private Funds Regulatory
UPDATE

# Treasury Makes It More Difficult for Ransomware Victims to Pay Ransoms

November 2020

On Oct. 1, 2020, the U.S. Department of the Treasury's Office of Foreign Assets Control ("OFAC") and the U.S. Department of the Treasury's Financial Crimes Enforcement Network ("FinCEN") each issued advisories on ransomware that, when taken together, make it more difficult for victims to lawfully pay ransoms to regain access to hijacked systems and recover stolen data.

The frequency of ransomware attacks has surged, as has the amounts cybercriminals demand. In the last quarter of 2019, the average ransom payment more than doubled from $84,116 to $190,946, with several organizations reporting seven-figure payments.[1] Navigating a ransomware attack has also become increasingly challenging as perpetrators develop more sophisticated means to infiltrate systems.

The OFAC advisory warns OFAC will impose sanctions on U.S. persons who engage in transactions (including making payments or facilitating payments) with individuals and entities involved in ransomware if they have appeared on OFAC's Specifically Designated Nationals and Blocked Persons List (an "SDN") or if they are covered by country or region embargoes. OFAC cautions that a U.S. person need not know that the recipient of payment has been designated because civil penalties may be imposed for sanctions violations based on strict liability (i.e., without knowledge the transaction was prohibited). This poses a significant risk when paying a ransom, as cybercriminals often disguise their identities when demanding payment, and ask for payment by digital currency, making it nearly impossible to determine whether a recipient has in fact been designated by OFAC.

The FinCEN advisory discusses predominant trends, typologies and potential red flag indicators of ransomware and associated money laundering activities and the related suspicious activity reporting requirements applicable to financial institutions. Specifically, FinCEN reminds financial institutions they may be required to file a SAR when dealing with an incident of ransomware.

The new advisories raise the familiar debate over "negotiating with terrorists." On one hand, paying ransoms makes ransomware attacks more lucrative for cyber criminals and encourages future attacks. On Oct. 13, member nations of the G-7 warned that perpetrators of ransomware attacks might be state-sponsored or linked actors who might use the ransom funds for further illicit purposes, such as

[1] The New York Times

funding weapons of mass destruction.[2] On the other hand, regulations that cause delays or impose prohibitions on paying ransoms inhibit what can be an economically efficient way for victims to respond to attacks and minimize the damage to their business continuity.[3]

For private equity sponsors and other fund managers that establish control positions, OFAC's new restrictions could have significant consequences for portfolio companies in certain subsectors, such as hospitals, that have been particularly hard hit by ransomware and have relied on ransom payments to avert attacks with devastating (and potentially deadly) consequences. In addition to potential sanctions from OFAC, G-7 officials have warned of additional coordinated sanctions applying across member nations.

The restrictions and other risks involved with ransom payments reinforce the importance of fund managers having plans in place to prevent and respond to ransomware attacks.[4] Fund managers should be familiar with the OFAC and FinCEN advisories and review them carefully if they become victims of ransomware. In the heat of the moment during a ransomware attack, it will be critical for the manager to determine if the ransom payment that is being demanded would violate applicable U.S. or non-U.S. law.

*This article appeared in the November 2020 edition of SRZ's Private Funds Regulatory Update. To read the full Update,* ***click here****.*

[2] Law360

[3] The Department of Justice ("DOJ") has also signaled an increased focus on the payment of ransoms and other interactions with cyber criminals. On Aug. 20, 2020, the former Chief Security Officer of Uber was indicted in federal court in California for obstruction of justice and misprision of felony in connection with the attempted cover-up of a 2016 hack, which included a ransom payment. The executive allegedly lied to the Federal Trade Commission, which was investigating a 2014 hack at the time the 2016 ransom was paid, and took efforts to conceal the ransom payment. The DOJ said the case should send a broader message about not concealing cybercrime: "While this case is an extreme example of a prolonged attempt to subvert law enforcement, we hope companies stand up and take notice. Do not help criminal hackers cover their tracks. Do not make the problem worse for your customers, and do not cover up criminal attempts to steal people's personal data."

[4] Our Aug. 17, 2020 *Alert* provides further information on the increasing risk of ransomware attacks, including steps that fund managers and financial institutions can take to increase preparedness for a cyber-attack.