4 Compliance Tips Amid Increased Ransomware Scrutiny

By **Colin Jennings, Ericka Johnson and Dylan Yépez** (October 8, 2020)

Colin Jennings

Ericka Johnson

Dylan Yépez

On Oct. 1, two bureaus of the U.S. Department of the Treasury, the Financial Crimes Enforcement Network and the Office of Foreign Assets Control, each published advisories providing that ransomware victims and any third-party companies involved in making ransom payments to persons under economic sanction may face civil penalties.

Given that these penalties are nothing new, the advisories likely signal a shift in the bureaus' joint efforts to increase oversight of ransomware payments.

Ransomware is a form of malicious software designed to block a company's access to its information technology environment, thus allowing threat actors to extort payments, i.e., ransom, in exchange for a decryption key allowing the company to regain access to its systems or data. In some cases, threat actors also steal company data and threaten to publish sensitive files if the company refuses to pay.

Unfortunately, it is generally more cost-effective for a company to pay a ransom, usually through a digital currency, than to restore the data itself. Likewise, the increasing prevalence of cyberinsurance allows threat actors to demand higher ransoms, knowing that an insurance carrier with deep pockets will bear the cost.

For these reasons, ransomware attacks have become more focused, sophisticated, costly and numerous, garnering greater attention from regulators such as OFAC and FinCEN, and likely prompting the bureaus to issue the recent advisories.

The advisories work in tandem to address these issues. The OFAC advisory sets forth the potential sanctions for victim companies and their third-party companies — e.g., financial institutions, cyberinsurance firms, digital-forensic and incident-response vendors — involved in making ransom payments.

The advisory reiterates that U.S. persons are prohibited from transacting with persons on OFAC's specially designated nationals and blocked persons list, other blocked persons, and those covered by the comprehensive country or region embargos, e.g., Cuba, Iran and North Korea. Those who do transact with prohibited persons may face a civil monetary penalty for violations.

FinCEN's advisory, in turn, sets forth the method by which the Treasury can be alerted to potentially illicit ransom payments. FinCEN's advisory reiterates financial institutions' obligations to report transactions concerning ransomware-related illicit activity through a suspicious activity report and details financial red-flag indicators of ransomware and associated payments. Upon receiving a suspicious activity report, FinCEN can further investigate whether the recipient was a prohibited person.

These advisory opinions place victim companies and their third-party response teams on

notice that their ransom payments will be subject to increased scrutiny. For that reason, this article provides the following practical implications and best practices for companies considering making a ransom payment.

1. OFAC checks need to be thoroughly analyzed and documented.

In responding to a ransomware attack, a victim company usually retains a vendor to liaise with the threat actor — who has courteously left their email address to be contacted for payment. The vendor, in turn, generally conducts due diligence on the threat actor's cryptocurrency wallet to ensure there is no affiliation with any prohibited persons. Given the Treasury bureaus' increased oversight, however, this may not suffice.

A victim company will usually also retain an IT vendor to conduct a forensic investigation to determine, among other things, the type of malware present in the company's IT environment and the potential affiliation of the malware with any known threat actors.

As a best practice, the IT vendor should also be involved in assisting the other vendor in conducting its due diligence. This means advising on whether the identified strain of malware is known or reasonably known to be associated or affiliated with a prohibited person.

Further, a victim company's outside counsel should clearly document the due diligence process and the bases for the determination of whether the threat actor has any known connection to prohibited persons. This will mitigate the risk of the company's paying a ransom to a prohibited person.

Remember, sanction violations are based on strict liability, meaning that a person can still be liable even if they did not know or have reason to know they were transacting with prohibited persons. A detailed analysis can mitigate the risk of committing sanctionable violations by ensuring that the due diligence is comprehensive and draws sound conclusions, thus reducing the likelihood that any connection to prohibited persons will be overlooked.

2. Review existing and potential cyberinsurance policies.

Generally, companies purchase cyberinsurance that will cover the cost of a ransom payment. OFAC's advisory makes clear, however, that even insurance carriers can be held civilly liable for payments to prohibited persons. For this reason, carriers will likely attempt to recoup from companies any civil fines for illicit payments. Companies should immediately review their current and pending insurance policies to determine whether they will require the companies to indemnify their carriers for any such civil liability.

As a practical matter, insurance companies will likely become more involved in the due diligence process to ensure that the threat actors are not prohibited persons and may be more risk averse where there is even the potential for an illicit payment. As a company must generally obtain prior permission from its carrier to make a ransom payment, this will likely become a contested area in the near future if carriers begin to deny coverage based on the mere potential for an illicit payment.

3. Add sanctions compliance to incident response plans.

The OFAC advisory opinion provides that in determining a company's civil fine, it will consider the existence, nature and adequacy of the company's sanctions compliance

program. Accordingly, companies should ensure that their incident response plans include protocols to conduct thorough due diligence on a threat actor prior to making any ransom payment.

A company's plan should also include a clear ban on any payments to prohibited persons and a mandate that the company notify law enforcement as appropriate. In the event of an attack, the company should be sure to strictly follow its sanctions-related compliance protocols and procedures. This will ensure that, should a violation nevertheless occur, OFAC will likely weigh the company's demonstrated compliance efforts in favor of a smaller civil penalty.

4. Consider notifying OFAC for sanctions nexus.

The OFAC advisory incentivizes companies to preemptively notify law enforcement in the event their due diligence uncovers a potential sanctions compliance concern. The advisory also encourages victims to contact OFAC and provides that a company's self-initiated, timely and complete report of a ransomware attack may be a significant mitigating factor in determining an appropriate enforcement outcome if a sanctions nexus is later discovered.

Generally, insurance policies require a company to notify law enforcement before paying a ransom. This typically includes making a notification to the Federal Bureau of Investigation.

Given that insurance companies may increasingly participate in the due diligence process, though, they may also request that companies report to OFAC if they believe that a request for ransomware payment may involve a sanctions nexus. Companies can thus mitigate their risk of sanctions violations and denial of coverage by erring on the side of contacting OFAC.

Ultimately, the legal analysis to determine whether a company can lawfully make a ransom payment and the business decision to do so are nuanced and complex, and, if you experience a data breach, it is best to retain counsel for guidance in determining whether, and if so how, to pay a ransom.

Colin Jennings is a partner, and Ericka Johnson and Dylan Yépez are associates, at Squire Patton Boggs LLP.

Squire Patton associate Elizabeth Weil Shaw contributed to this article.