SAUL EWING ARNSTEIN & LEHR LLP

ALERT

Cybersecurity and Privacy Practice
White Collar and Government Litigation Practice

OCTOBER 2020

Paying or Facilitating Payment of Ransomware Demands May Result in Criminal and Civil Penalties From OFAC

Laurie A. Kamaiko | Joseph A. Valenti | Christie R. McGuinness

Companies that make or facilitate ransomware payments were given a strong reminder of their due-diligence and compliance obligations by the U.S. Department of the Treasury's Office of Foreign Assets Control ("OFAC"). OFAC's recent October 1, 2020 advisory (the "Advisory") noted that all entities involved in the chain of facilitating ransomware payments—from victim companies, company executives/employees, forensic vendors, incident-response firms that advise victims, cyber insurers that insure such payments, and the financial institutions[1] (including cryptocurrency exchanges and money-services businesses) that may be involved in processing ransom payments—may all be at risk of criminal and civil penalties under the laws administered by OFAC if they do not exercise appropriate due diligence and have in place compliance procedures to ensure that payments do not go to any entity on U.S. sanctions lists. This alert will discuss the Advisory and how companies can follow the path to compliance.

What's Ransomware and Why Is OFAC Concerned?

As noted in the Advisory, "[r]ansomware is a form of malicious software ('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…The cyber 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." [2]

Ransomware attacks have escalated in both frequency and severity (the amounts demanded) in the past few years according to FBI reports cited in the Advisory, with incidents increasing even further during the COVID-19 pandemic as businesses increased their reliance on online systems.[3] This escalation, in turn, led OFAC to "highlight the sanctions risks associated with ransomware payments related to malicious cyber-enabled activities" and increase awareness that payments made to sanctioned entities or jurisdictions could be used to fund activities adverse to American national security and foreign policy, fund other illicit aims, or fund further attacks.

Several of the most destructive ransomware operators are presently sanctioned by OFAC. OFAC updates its sanctions frequently, particularly when new cyber threats emerge from China, Iran, North Korea, Russia, other countries, or organized non-state actors. Because the identity of perpetrators of ransomware attacks are usually not known or identifiable, OFAC is concerned that ransom payments are funneling into the coffers of entities and jurisdictions on their sanctions list, to be used against U.S. interests, and to fund further attacks.

Thus, OFAC is reminding entities involved in facilitating ransomware payments that "if there is a reason to believe the cyber actor demanding ransomware payment may be sanctioned or otherwise ha[s] a sanctions nexus," then those entities may be violating OFAC regulations and be subject to OFAC-imposed penalties.

What's the Specially Designated Nationals ("SDN") and Blocked Persons List (the "Sanctions List")?

The Sanctions List is the who's who list of perceived bad actors with whom U.S. persons are "prohibited from engaging in transactions, directly or indirectly[.]" The Sanctions List includes "individuals or entities [named as SDNs], other blocked persons, and those covered by comprehensive country or region embargoes." Some examples of countries/areas subject to broad sanctions are Cuba, the Crimea region of Ukraine, Iran, North Korea, and Syria. Payments to anyone on the Sanctions List—or even to certain regions—are presumptively illegal and require either an analysis that shows a general license applies to authorize the payment or obtaining a specific license where OFAC grants permission to engage in a certain transaction. One of the risks of making a ransomware payment is that the payment is going to a sanctioned country or entity, particularly when the payment is made quickly, covertly, and/or through intermediaries.

What Are the Consequences of Engaging in a Transaction With an Entity on the Sanctions List?

The Advisory warns that "OFAC may impose civil penalties for sanctions violations based on strict liability, meaning that a person subject to U.S. jurisdiction may be held civilly liable even if it did not know or have reason to know it was engaging in a transaction with a person that is prohibited under sanctions laws and regulations administered by OFAC." When an entity makes or facilitates a ransomware payment to a sanctioned entity, the violation is complete.[4] Mental state, knowledge, duress, and other typical elements or affirmative defenses are not legally available.

An appeal to prosecutorial discretion and OFAC's sensibilities must be made to obtain lenient treatment, which often raises the question of why OFAC input or licensing was not sought before payment was made in these contexts[5]. Strict liability thus provides significant leverage to OFAC, which companies must carefully consider when facilitating ransomware payments.

Of course, criminal penalties for reckless or willful violations of the sanctions laws also exist. Depending on the specific sanctions law at issue, prison terms up to 20 years may be handed down to individuals in addition to $1,000,000 corporate fines, along with massive forfeiture orders that can seize any property used to facilitate the violation.

The Advisory's Guidance to Companies

The Advisory identifies actions that companies can implement to aid them in avoiding enforcement from the Treasury Department.

Before a ransomware issue even arises, the Advisory "encourages" implementation of a "risk-based compliance program to mitigate exposure to sanctions-related violations." It notes that, under OFAC's Enforcement Guidelines, in the event of an apparent violation of U.S. sanctions law or regulations, factors OFAC may consider in determining its enforcement response include the existence, nature, and adequacy of a sanctions compliance program. The Advisory specifically identifies entities involved in providing cyber insurance, digital forensic and incident response, and financial services that may involve processing ransom payments (including depository institutions and money-services businesses), as entities that should consider such compliance programs. The Advisory suggests that such programs:

- Account for the risk that a ransomware payment may involve an SDN, blocked person, or a comprehensively embargoed jurisdiction.
- Consider whether the entity has additional regulatory obligations under FinCEN (relating to monitoring for and reporting suspicious activity).
- Consider OFAC's 2019 issuance of "A Framework for OFAC Compliance Commitments." In it, OFAC identified five (5) major areas for compliance: Management Commitment, Risk Assessment, Internal Controls, Testing and Auditing, and Training.

The Advisory further notes that OFAC will also consider a company's "self-initiated, timely, and complete report of a ransomware attack to law enforcement" and its cooperation with law enforcement during and after a ransomware attack to be a "significant mitigating factor" in determining an appropriate enforcement outcome if the situation is later determined to have a sanctions nexus.

Finally, the Advisory also reminds companies that they can seek a license (in essence, pre-payment permission) to perform the requested financial transaction. Even taking the effort to verbally notify OFAC or complete its online form before making a time-sensitive payment demonstrates an effort to recognize the balance between national security and vital economic and operational interests (and, in some cases—like medical centers—lifesaving data restoration).

Conclusion

It is significant that the Advisory applies to all entities involved in the facilitation of ransomware payments, not just the victim of the ransomware attack who authorizes the ransom payment. OFAC reminds everyone that legal violations both trace back to the source (*e.g.*, a victim that cannot shield itself by authorizing indirectly what it cannot do directly) and follow downstream (*e.g.*, entities such as law firms, forensic vendors, cybersecurity advisors, insurers, and banks that may assist victims of ransomware attacks). It is clearly trying to encourage all involved in the decision-making and payment chain to undertake due diligence and fully implement a sanctions compliance program.

The Advisory emphasizes the importance of these entities having their own appropriate compliance program that, among other things, establishes a procedure in advance for determining and assessing the risk that the recipient of a ransomware payment is on or associated with an entity or jurisdiction on the Sanctions List. OFAC also expects companies to provide employees with clear directives on how to respond to ransomware attacks. Companies should also be in a position to comprehensively document and walk the government through their compliance programs and responses to ransomware attacks. The Advisory indicates that OFAC will be scrutinizing the compliance programs as a significant factor in determining whether OFAC pushes a transaction toward the path of enforcement and penalties.

The Advisory encourages early, full consultation with law enforcement, OFAC, and FinCEN. The Advisory makes it clear that this voluntary disclosure is a significant factor that will be analyzed when determining whether to seek enforcement. While ransomware perpetrators often seek to force their victims into quick, covert payments, the United States government—through the coordinated guidance issued by its agencies within the Treasury Department—makes clear its stance that efforts to avoid detection and keep law enforcement in the dark aid these perpetrators—and may be investigated and prosecuted as such. Indeed, the mischaracterization of a ransomware payment on legal documents, accounting records, or statements to government officials may create separate avenues for liability.

The Advisory also indicates the importance of a victim of a ransomware attack using vendors and advisors knowledgeable about the risk of violation of OFAC requirements. The Advisory may be a harbinger not only of increased scrutiny by OFAC on involved entities, but also of increased scrutiny by entities in the chain of payments on each other to ascertain if due diligence and compliance with sanctions programs has been followed. Moreover, going forward, there may be increased pressure by all in the payment chain on policyholders and their vendors to reach out to law enforcement, perhaps even to open routine lines of communication before the urgency of a ransomware attack even exists. Companies seeking cyber insurance may see an increase in questions by insurers directed at determining if the policyholder has an appropriate compliance program. In addition, any entity meeting the broad definition of "financial institution" in the Bank Secrecy Act's implementing regulations have additional responsibilities, such as following "Know Your Customer/Client" requirements, meeting anti-money-laundering compliance expectations, and reporting suspicious activity.

Consultation with well-trained lawyers and cybersecurity consultants ahead of any ransomware attacks are typically prudent measures that can dramatically reduce both the risks of attacks and the costs of responding to attacks.

Overall, the message in the Advisory is that, in this environment of increasing ransomware attacks on companies in all industries, all companies should understand and be prepared to be compliant with OFAC regulations, before that attack occurs.

---

1. The United States Treasury's Financial Crimes Enforcement Network ("FinCEN") also published its own advisory on October 1, 2020 that is focused on how to detect suspicious activity from a financial institution's perspective (particularly when a customer or vendor is trying to conceal that a ransom payment is being made). . . . It discusses how financial institutions subject to the Bank Secrecy Act's suspicious-activity-reporting requirements may tailor compliance programs to detect and report red flags that often indicate that an entity is surreptitiously using its services to facilitate a ransomware payment. OFAC's guidance is perhaps more applicable when the existence of a ransomware demand or payment is known rather than simply speculated, and the legality of the payment itself is in question (as opposed to the legality of reporting or not reporting the payment via a suspicious activity report). *See* FIN-2020-A006 at https://www.fincen.gov/sites/default/files/advisory/2020-10-01/Advisory Ransomware FINAL 508.pdf
2. All quotes are to the Advisory unless otherwise indicated.
3. Moreover, on July 30, 2020, FinCEN released an advisory indicating that it had seen an increase in ransomware through phishing emails with the subject CARES ACT in the subject line. FinCEN also indicated that it saw an increase in suspicious activity reports noting that ransomware attacks were being directed at medical centers and municipalities.
4. For examples of broad sanctions regulations prohibiting payments without a mens rea requirement, *see, e.g.*, 31 C.F.R. § 560.208 ("[N]o United States person, wherever located, may approve, finance, facilitate, or guarantee any transaction by a foreign person where the transaction by that foreign person would be prohibited by this part [of the U.S.-Iranian sanctions law] if performed by a United States person or within the United States."); 31 C.F.R. § 560.211(c)(1)(i) ("All…interests in property…within the possession or control of any United States person…of the following persons are blocked and may not be transferred, paid, exported, withdrawn, or otherwise dealt in[:] Any person determined by the Secretary of the Treasury…to be owned or controlled by…any person whose property and interests in property are blocked[.]").
5. *See* 31 C.F.R. part 501, appx. A.

This alert was written by Laurie A. Kamaiko, Joseph A. Valenti, and Christie R. McGuinness. Laurie is Chair of the Firm's Cyber Insurance Practice and can be reached at (212) 980-7202 or at Laurie.Kamaiko@saul.com. Joe is a member of the Firm's Cybersecurity and Privacy Practice and can be reached at (412) 209-2569 or at Joe.Valenti@saul.com. Christie is a member of the Firm's White Collar and Government Litigation Practice and can be reached at (212) 980-7205 or at Christie.McGuinness@saul.com. This alert has been prepared for information purposes only.

Did you find this information useful? Please provide your feedback here and also let us know if there are other legal topics of interest to you.