October 2, 2020

Between a Rock and a Hard Place: OFAC Issues Advisory on Ransomware Payments

Attorneys
Ama A. Adams
Brendan C. Hanifin
Emerson Siegle

On October 1, the U.S. Department of the Treasury's Office of Foreign Assets Control ("OFAC") published an advisory to alert companies on potential sanctions risks related to ransomware payments (the "Advisory").[1] While ransomware attacks, by design, create business-critical problems requiring swift attention and remediation, the Advisory cautions that victims of ransomware attacks, and ransomware-related services providers, must balance such considerations against the risk of sanctions liability.

Background

As described in the Advisory, ransomware is a form of malicious software 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 recent years, the volume of ransomware attacks targeting U.S. companies has surged, and the COVID-19 pandemic has accelerated this trend.

Payment of ransomware demands by U.S. persons and companies can present sanctions risk where the attack is suspected of originating from a sanctioned jurisdiction or sanctioned party.[2] U.S. companies that fall victim to such ransomware attacks thus face a dilemma: (1) refuse the demand, in some cases with catastrophic commercial consequences; or (2) pay the demand without OFAC authorization, in potential violation of U.S. sanctions. Further, because U.S. sanctions are a strict liability regime, uncertainty regarding the origin of the attack may not provide a viable defense in the event OFAC were to initiate an enforcement action.

Notably, this risk is not limited to U.S. companies that fall victim to ransomware demands, for several reasons:

- First, the U.S. sanctions regulations prohibit covered parties from facilitating transactions by third persons that involve sanctioned countries or sanctioned parties. As such, firms subject to U.S. jurisdiction that offer ransomware negotiation services or insurance products—as well as financial institutions that process ransomware payments—risk engaging in impermissible facilitation of the victim's ransomware payment to a prohibited party.[3]

- Second, certain U.S. sanctions authorities authorize OFAC to impose sanctions on non-U.S. parties—not ordinarily subject to OFAC's jurisdiction—that provide financial, material, or technological support to sanctioned parties (which may include sanctioned cyber-actors). As such, even non-U.S. companies that accede to ransomware demands, at least in theory, could face U.S. sanctions risk.

Advisory

The Advisory confirms that ransomware payments to sanctioned parties or jurisdictions, where the transaction involves a U.S. jurisdictional nexus, may violate U.S. sanctions, and subject the payer—as well as any parties who facilitate the payment—to civil penalties. Notably, the Advisory emphasizes the strict liability nature of the sanctions regulations, seemingly to emphasize that the payment of ransomware demands, even where there is no identified connection to a sanctioned party or country, may ultimately be deemed a violation of U.S. sanctions (if such a connection is later identified):

> 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

ATTORNEY ADVERTISING

> engaging in a transaction with a person that is prohibited under sanctions laws and regulations administered by OFAC.

Advisory at 3.

Many companies faced with the ransomware dilemma have reasoned that, in assessing whether to pursue an enforcement action over payment of the ransom, OFAC would consider mitigating factors, such as the culpability of the cyber-actor (as compared to the victim), the consequences of non-payment to the victim, and the inability to determine definitively the origin of the attack.

The Advisory suggests that OFAC would place limited, if any, weight on these collateral considerations. Instead, the Advisory emphasizes that OFAC will consider the following, alternative considerations as "significant mitigating factors"—in addition to the existence, nature, and adequacy of the victim's sanctions compliance program—in determining the appropriate enforcement outcome:

- the victim's self-initiated, timely, and complete report of a ransomware attack to law enforcement;[4] and
- the victim's full and timely cooperation with law enforcement both during and after a ransomware attack.

Although the Advisory does not state so specifically, where a ransom is paid, OFAC presumably would take the position that payment significantly undermined the objectives of its sanctions programs, an aggravating factor in assessing the appropriate enforcement outcome.[5]

In view of the above, a U.S. company facing a ransomware demand logically might consider the option of seeking a specific license from OFAC authorizing payment. However, the Advisory makes clear that specific license applications involving ransomware payments "will be reviewed by OFAC on a case-by-case basis with a presumption of denial." This policy, in conjunction with the enforcement factors identified above, suggests that victims of ransomware attacks may need to weigh the commercial costs of non-payment against the likelihood of an enforcement action, with no precedent from which to assess the posture OFAC might take in the latter circumstance.

Conclusion

The Advisory confirms the concerns of many sanctions practitioners with respect to OFAC's enforcement posture. In particular, although OFAC apparently recognizes the dilemma facing ransomware victims, exigent circumstances do not relieve victims of their sanctions compliance obligations. Further, as OFAC continues to designate malicious cyber-actors, the scope of ransomware attacks involving a U.S. sanctions nexus foreseeably will increase.

Over the coming weeks and months, we will be monitoring whether the Advisory is a precursor to sanctions enforcement against parties who pay (or facilitate payment of) ransomware demands.

1. On the same day, the Financial Crimes Enforcement Network ("FinCEN"), also housed within the Treasury Department, published a companion advisory to alert financial institutions to predominant trends, typologies, and potential indicators of ransomware and associated money laundering activities.
2. In recent years, OFAC has been increasingly aggressive in designating malicious cyber-actors.
3. Notably, in its separate advisory, FinCEN indicated that certain digital forensics and incident response companies ("DFIRs"), cyber insurance companies ("CICs"), and certain money services businesses ("MSBs") that offer convertible virtual currencies ("CVCs") "facilitate ransomware payments to cybercriminals, often by directly receiving customers' fiat funds, exchanging them for CVC, and then transferring the CVC to criminal-controlled accounts." FinCEN warned that "this activity could constitute money transmission," which would require the DFIRs and CICs to register as MSBs with FinCEN and comply with anti-money laundering obligations pursuant to the U.S. Bank Secrecy Act. However, depending on the circumstances, this activity—acting to "facilitate" payments to certain criminals—could also represent a violation of U.S. sanctions.

ATTORNEY ADVERTISING

4. In this regard, the Advisory states, "OFAC encourages victims and those involved with addressing ransomware attacks to contact OFAC immediately if they believe a request for a ransomware payment may involve a sanctions nexus."
5. Companies that decline to pay a ransomware demand for sanctions-related reasons must consider whether the decision triggers an affirmative OFAC reporting requirement under the Reporting, Procedures and Penalties Regulations ("RPPR"), 31 C.F.R. § 501 *et seq*. The RPPR require all covered parties—including non-financial institutions—to timely report rejected transactions to OFAC.

This alert should not be construed as legal advice or a legal opinion on any specific facts or circumstances. This alert is not intended to create, and receipt of it does not constitute, a lawyer-client relationship. The contents are intended for general informational purposes only, and you are urged to consult your attorney concerning any particular situation and any specific legal question you may have. © 2020 Ropes & Gray LLP

ATTORNEY ADVERTISING