New York Law Journal
SERVING THE BENCH AND BAR SINCE 1888
WWW.NYLJ.COM
An ALM Publication
VOLUME 265—NO. 42
MONDAY, MARCH 8, 2021

Outside Counsel

Don't Blame the Victim: A Potential Defense for Ransom Payers and Facilitators after OFAC's Ransomware Sanctions Facilitation Advisory

By **Michael A. Kleinman**

And **Marc Schein**

In October 2020, the Department of Treasury's Office of Foreign Assets Control (OFAC) issued an "Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments" (the Advisory), putting into writing guidance to reinforce the prohibition of ransom payments by ransomware attack victims to not only the defined class of Specially Designated Nationals (SDNs) targeted under Treasury's Cyber Sanctions Program—but also to a broad class of *any* entities with a "sanctions nexus" to SDNs. The Advisory, however, does not contain any insight into just what constitutes a "sanctions nexus" in the unique context of Treasury's Cyber Sanctions Program. Nevertheless, the Advisory memorializes OFAC's ability to impose strict liability on any company that makes the difficult decision to pay a ransom to protect its reputation, business secrets, personal data, and value for shareholders. What is more, the Advisory also specifically warns the ransom negotiators, insurers, and financial institutions that assist victims who make the difficult decision to pay that they, too, may be liable for facilitating a ransom payment with the undefined "sanctions nexus."

There are plenty of good reasons not to pay a ransom, not least of which is the lack of any guaranty that a threat actor will simply disappear, never to return. But in many instances, without paying, management will be unable to run its business or deliver its goods and services. The decision not to pay can be devastating. For example, when a SamSam attack hit the City of Atlanta in March 2018 (an incident referenced in the Advisory), the City elected not to pay the $51,000 demanded for decryption. The result was an inability to work around the encryption and a cost of $17 million to rebuild its network.

> At least one company recently succeeded in a judicial challenge to sanctions enforcement based on OFAC's failure to provide fair notice of what constituted sanctionable conduct under one of its (non-cyber) regulations.

Ignoring such real world consequences, the Advisory's reminder that OFAC imposes strict liability for payments to those with an undefined "sanctions nexus" coupled with the unique inability to identify all prohibited individuals and the digital currency accounts they use to receive a ransom leaves ransomware victims, who desperately need the comfort of certainty after an attack, with no comfort at all.

While many commentators have reacted to the Advisory by stressing the importance of implementing robust screening and compliance measures and warning companies to do their best to avoid paying ransoms, we focus on how to mount a defense to a potential sanctions enforcement action under the Advisory when some or all of those efforts have been taken to no avail.

Background Leading Up to OFAC's October 2020 Ransomware Advisory. In response to the proliferation of ransomware attacks over the last five years in particular, a series of Executive Orders and statutes, as further codified by OFAC in its regulations and

MICHAEL A. KLEINMAN *is a special counsel of Fried, Frank, Harris, Shriver & Jacobson.* MARC SCHEIN, *CIC, CLCS, is the National Co-Chair, Cyber Center of Excellence at Marsh & McLennan Agency.* BRYAN A. McINTYRE, *an associate at Fried Frank, assisted in the preparation of this column.*

explained in advisories, have come to include cyberterrorists amongst the list of banned individuals with whom U.S. persons cannot conduct financial transactions. See, e.g., U.S. Dep't of Treas., *Sanctions Related to Significant Malicious Cyber-Enabled Activities*.

In 2015, President Obama issued Executive Order 13694 (E.O. 13694) titled "Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities," which, among other things, authorized the imposition of sanctions against any person responsible for or complicit in, directly *or indirectly*, engaging in "malicious cyber-enabled" activities that are "reasonably likely to result in, or have materially contributed to, a significant threat to the national security … of the United States." The list of cyber activity subject to sanctions is incredibly broad in scope and includes: "causing a significant disruption to the availability of a computer or network(s) of computers; [ ] causing a significant misappropriation of funds or economic resources, trade secrets, personal identifiers, or financial information;" or any other activity that disrupts computer infrastructures or threatens access to an entity's vital information. 80 Fed. Reg. 18077 (April 1, 2015).

In accordance with E.O. 13694, Treasury implemented its "Cyber-Related Sanctions Regulations" (31 C.F.R. §§578 et seq.) on Dec. 31, 2015 (the Regulations), giving birth to OFAC's Cyber Sanctions Program. As is common for "list-based" sanctions programs, the Regulations offered little interpretative guidance to E.O. 13694's broad language, merely incorporating the E.O. by reference. Nor has any subsequent guidance issued by Treasury provided any more clarity until the Advisory.

For example, the 15 Cyber-Related FAQs maintained on Treasury's website as of Feb. 2, 2021 focus on: developing a tailored, risk-based compliance program that *may* include screening "or other appropriate measures;" clarifying certain exclusions from the Regulations, such as American whistleblower activity, provision of legal advice, and network defense; and noting that a general license allows certain transactions with the Russian Federal Security Service. Notably, despite the acceleration of ransomware attacks in the last few years, there has been no new Cyber-Related FAQ posted since November 2018. See U.S. Dep't of Treas., *Frequently Asked Questions, Cyber-Related Sanctions*.

> There are plenty of good reasons not to pay a ransom, not least of which is the lack of any guaranty that a threat actor will simply disappear, never to return. But in many instances, without paying, management will be unable to run its business or deliver its goods and services. The decision not to pay can be devastating.

Aside from the Advisory and the FAQs, the only other guidance published by Treasury on its Cyber-Related Sanctions Program is a document entitled "Sanctions Against Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities," which was last updated in July 2017 (the Guidance"). In large part, the Guidance merely summarizes existing authorities and potential penalties. There are, however, two notable highlights. First, the Guidance itself characterizes the Regulations as "abbreviated" but states that "OFAC intends to supplement the Regulations with a more comprehensive set of regulations, which may include additional interpretative and definitional guidance and additional general licenses and statements of licensing policy." Yet no supplemental regulations have been implemented. Second, the Guidance states that special licenses to authorize otherwise banned transactions will be considered on a case-by-case basis, but does not provide any criteria for how to make a decision.

In light of the limited guidance and dearth of specific regulations covering OFAC's Cyber Sanctions Program, word of the October 2020 Advisory should have been welcome news to the cyber and international trade communities. Unfortunately, however, the Advisory created more questions than it answered.

How Companies Should Think About the Advisory. Coming on the heels of an increase in demand for ransomware payments during the COVID-19 pandemic, the Advisory signals OFAC's intent to more actively regulate the flow of funds to threat actors out of a fear that those who perpetrate the attacks may be using the proceeds to fund "activities adverse to the national security and foreign policy objectives of the United States." But it is not just victims that need be concerned. The Advisory also specifically calls out financial institutions, cyber insurance firms, and companies involved in digital forensics and incident response for encouraging future ransomware payment demands by helping victims pay to recover access to their data.

The Advisory reiterates that OFAC has the authority to issue civil penalties to and refer for criminal investigation and/or prosecution under the International Emergency Economic

Powers Act and the Trading With the Enemy Act *any* companies negotiating ransomware payments with those "designated [as] malicious cyber actors under [OFAC's] cyber-related sanctions program," as well as those who have a *"sanctions nexus"* to these actors. But the number of cyber actors on the SDN list, particularly when considering the undefined "sanctions nexus," is truly unknowable. As of Jan. 19, 2021, the SDN list includes at least 130 known cyber threat actors, generally with one or more digital currency wallet addresses. But this list is just the tip of the iceberg of those who move below the surface on the Dark Web. Anonymous threat actors are notorious for working in groups or syndicates with other individuals or affiliates. And worse yet, in the last few years, "Ransomware as a Service" offered by several notorious syndicates has served to create a diaspora of unknown threat actors who buy or lease ransomware variants to deploy their own attacks.

Put simply, while there is a long list of threat actors and wallet addresses that companies can screen to determine if they can proceed with payment, the Advisory's addition of those individuals who post hoc are found by OFAC to have had a "sanctions nexus" to an SDN adds to the list of prohibited individuals a group of threat actors that would have slipped through reasonable screening programs maintained by victims and their advisors. Indeed, if OFAC later determines that the threat actor was an SDN, otherwise blocked, or located in a sanctioned country, the victim and its advisors will have violated the Regulations regardless of *any* screening the victim performed.

Victims who have run the screens and followed responsible incident response plans, yet still pay actors later deemed to have a sanctions nexus to a blocked entity by OFAC, thus will be put in an impossible situation: Don't pay and risk potentially material operational, reputational, and monetary consequences, or roll the dice and pay the perpetrator, then potentially pay OFAC again after innocently entering the unknown realm of the "sanctions nexus" (and *still* risk potentially material operational, reputational, and monetary consequences).

While the Advisory makes clear that credit will be given to those ransom payers who undertake mitigation efforts such as maintaining robust compliance programs and making self-initiated, timely, and complete reporting of an attack to law enforcement, the Advisory does not provide any clarity on how such mitigation efforts will avoid fines for payments involving the "sanctions nexus" other than to say that notification and cooperation with law enforcement will be seen as "significant."

On the other hand, what is clear from the Advisory is that a "specific" OFAC license, which would bless an otherwise unlawful payment, is all but foreclosed. First, the Advisory states that any license application will be met with a "presumption of denial." Second, in any event, since the typical victim has a matter of days to decide to pay a ransom and the OFAC license application process can take weeks or months, an OFAC license is for all intents out of the question.

One collateral effect of the Advisory's specific warning to cyber insurers who assist victims who decide to pay ransoms may be an increase in coverage denials for ransom payments made by or on behalf of insureds. It is critical that management understands how the company's cyber insurance policies may respond to a ransomware event. In particular, management must understand the difference between the "pay on behalf of" and "reimbursement" clauses in their cyber insurance policies. As ransomware attacks have escalated in the recent past, ransom demands exceeding $1 million have become commonplace, with some demands exceeding $10 million. This is also evidence showing that average ransom payments across all industries increased in the third quarter of 2020, and that cyber insurance claims are rising drastically. Increased regulatory scrutiny signaled by the Advisory combined with the increase in ransomware attacks may lead to an elimination of the "pay on behalf of" option, resulting in a large out of pocket expense that not all businesses can afford. Moreover, the new "sanctions nexus" language in the Advisory may vitiate coverage for OFAC penalties and related losses under a reimbursement clause altogether, when coupled with a sanctions limitation or exclusion clause. Indeed, the cyber insurance market has already tightened in response to the uptick in ransomware claims. Carriers are now requiring supplemental coverage applications to procure ransomware and cyber extortion insurance, and putting in place sublimits for such coverage parts. What is more, several carriers have left the market altogether. Finally, on Feb. 4, 2021, the New York State Department of Financial Services issued an Insurance Circular Letter addressed to all property and casualty insurers, citing the Advisory and an increase in ransomware incidents, and warning insurers that they too can be liable for ransom payments made to sanctioned entities. The letter set forth a new Cyber Insurance Risk Framework outlining best practices

that insurers who write cyber insurance policies should take to manage more effectively their own risks to potentially "massive" claim losses.

Can Companies Defend Themselves Against the 'Sanctions Nexus'? Whether or not a ransom payment is ultimately covered by insurance, what defense is available to a victim or facilitator who has run the screens, attempted the mitigating factors suggested by OFAC, and made the difficult decision to pay a non-SDN threat actor that nevertheless later turns up to have a "sanctions nexus"?

At least one company recently succeeded in a judicial challenge to sanctions enforcement based on OFAC's failure to provide fair notice of what constituted sanctionable conduct under one of its (non-cyber) regulations. In *Exxon Mobil v. Mnuchin*, Exxon filed an action against the Secretary of the Treasury and OFAC challenging a $2,000,000 fine imposed on Exxon for doing business with a non-SDN company, whose president and chairman had been designated as an SDN "in his individual capacity." 430 F. Supp. 3d 220, 226 (N.D. Tex. 2019). There, Exxon's entry into a series of contracts with the company, signed by the SDN, as president, without seeking preapproval from OFAC was deemed to be prohibited conduct.

The regulation at issue in *Exxon* provided that a U.S. company could not receive "services" from individuals or entities identified on OFAC's SDN list. Exxon asserted that OFAC's failure to define "receipt of services" was a violation of the Due Process Clause of the Fifth Amendment. Id. at 229. In response, OFAC contended that Exxon clearly received services from a SDN because the SDN signed the contracts on behalf of the company, and the signature of the SDN clearly constituted the receipt of services from the SDN. Id. at 231-32.

Noting that "fair notice" in the administrative agency context required OFAC to provide "'ascertainable certainty' of its interpretation of the Regulations," the court found that neither the Regulations nor any other OFAC guidance served to put Exxon on notice that the SDN's execution of the contract in his corporate capacity would constitute a "receipt of services." Id. at 233. Clearly recognizing the inherent vagaries in that sanctions program, the court colorfully framed the issue as a determination of "which party receive[d] the benefit of having its cake and eating it, too—the regulating agency that failed to clarify, or the regulated party that failed to ask." Id. at 225.

In the cyber context, the vague description of "sanctions nexus," which is absent from the Executive Orders, the FAQs, and the Guidance, does not clear the ultimate hurdle of "ascertainable certainty" required by the Fifth Amendment. That is, just as OFAC sought to justify an enforcement action based on the "receipt of services" language in *Exxon*, any finding of liability for payments to a non-SDN based on the cyber Regulations would force OFAC to justify cyber-related sanctions based on undefined "sanctions nexus" language. To date, the term "sanctions nexus" is *only* contained in the Advisory, and OFAC purports to define fully the term in a matter of a few sentences in the Advisory containing non-exhaustive hypotheticals. In *Exxon*, the court rejected OFAC's argument that the "sweeping language" it used had a "common meaning" that justified sanctions despite the absence of any public statements clarifying its meaning. Id. at 232. The Advisory and the scant additional public statements by OFAC on its Cyber Sanctions Program should fair no better when subject to judicial scrutiny. That is, a court applying *Exxon* to the "sanctions nexus" language should likewise hold that the Regulations are vague, overly "broad," and that the OFAC guidance "fails to delineate their boundaries." Id. at 243.

Accordingly, *Exxon* can well serve as a roadmap for a defense to sanctions enforcement against a ransomware victim and its advisors premised on nothing other than a "sanctions nexus." While the *Exxon* decision is far from precedential given it represents just one district judge's opinion in the very rare occasion where a party challenged OFAC sanctions in district court—let alone successfully, it provides a path to a potential defense for victims and their advisors who make the difficult choice to work together to pay an unknown threat actor.