The Sedona Conference Journal

Volume 25 2024

Commentary on U.S. Sanctions-Related Risks for Ransomware Payments

The Sedona Conference

Recommended Citation:

The Sedona Conference, *Commentary on U.S. Sanctions-Related Risks for Ransomware Payments*, 25 SEDONA CONF. J. 617 (2024).

For this and additional publications see: https://thesedonaconference.org/publications.

COMMENTARY ON U.S. SANCTIONS-RELATED RISKS FOR RANSOMWARE PAYMENTS

A Project of The Sedona Conference Working Group on Data Security and Privacy Liability (WG11)

Author:

The Sedona Conference

Editor-in-Chief:

Jim Shook

Contributing Editors:

John Gray
Eric B. Gyasi
Bill Hardin
Emily Jennings
Robert Kirtley
Jon Polenberg
Daniel E. Raymond
W. Lawrence Wescott
Zachary Willenbrink
Philip N. Yannella

Steering Committee Liaison

Alfred J. Saikali

Staff Editors:

David Lumia
Michael Pomarico

The opinions expressed in this publication, unless otherwise attributed, represent consensus views of the members of The Sedona Conference Working Group 11. They do not necessarily represent the views of any of the individual participants or their employers, clients, or any other organizations to which any of

the participants belong, nor do they necessarily represent official positions of The Sedona Conference.

We thank all of our Working Group Series Annual Sponsors, whose support is essential to our ability to develop Working Group Series publications. For a listing of our sponsors, just click on the "Sponsors" navigation bar on the homepage of our website.

This publication may be cited as follows:

> The Sedona Conference, *Commentary on U.S. Sanctions-Related Risks for Ransomware Payments*, 25 SEDONA CONF. J. 617 (2024).

PREFACE

Welcome to the October 2024 final version of The Sedona Conference's *Commentary on U.S. Sanctions-Related Risks for Ransomware Payments* ("*Commentary*"), a project of The Sedona Conference Working Group 11 on Data Security and Privacy Liability (WG11). This is one of a series of Working Group commentaries published by The Sedona Conference, a 501(c)(3) research and educational institute dedicated to the advanced study of law and policy in the areas of antitrust law, complex litigation, intellectual property rights, and data security and privacy law. The mission of The Sedona Conference is to move the law forward in a reasoned and just way through dialogue and consensus.

The mission of WG11 is to identify and comment on trends in data security and privacy law, in an effort to help organizations prepare for and respond to data breaches, and to assist attorneys and judicial officers in resolving questions of legal liability and damages.

The Sedona Conference acknowledges Editor-in-Chief Jim Shook for his leadership and commitment to the project. We also thank contributing editors John Gray, Eric Gyasi, Bill Hardin, Emily Jennings, Robert Kirtley, Jon Polenberg, Daniel Raymond, Larry Wescott, Zach Willenbrink, and Phil Yannella for their efforts. We also thank Al Saikali for his contributions as Steering Committee liaison to the project and Guillermo Christensen for his contributions.

In addition to the drafters, this nonpartisan, consensus-based publication represents the collective effort of other members of WG11 who reviewed, commented on, and proposed edits to early drafts of the *Commentary* that were circulated for feedback from the Working Group membership. Other members provided feedback at WG11 annual and midyear meetings

where drafts of the *Commentary* were the subject of the dialogue. The publication was also subject to a period of public comment. On behalf of The Sedona Conference, I thank all of them for their contributions.

We encourage your active engagement in the dialogue. Membership in The Sedona Conference Working Group Series is open to all. The Series includes WG11 and several other Working Groups in the areas of electronic document management and discovery, cross-border discovery and data protection laws, international data transfers, patent litigation, patent remedies and damages, trade secrets, and artificial intelligence. The Sedona Conference hopes and anticipates that the output of its Working Groups will evolve into authoritative statements of law, both as it is and as it should be. Information on membership and a description of current Working Group activities is available at https://thesedonaconference.org/wgs.

Kenneth J. Withers
Executive Director
The Sedona Conference
October 2024

TABLE OF CONTENTS

I. INTRODUCTION

Threat actors, using ransomware attacks,[1] are preying on computer networks of organizations worldwide. Utilizing malware and other tools, threat actors encrypt both data and applications and prevent access to an organization's cyber network, causing an abrupt stop to, material disruption of, or significant degradation in an organization's ability to conduct business. These threat actors demand a ransomware payment in return for a decryption tool used to regain network access and increasingly also attempt to extort ransomware victims by threatening to publicize stolen data. Ransomware attacks can result in substantial costs, serious disruptions to essential services and supply chains, and even risks to life. Determining whether to pay a ransom or work to recover systems without access to the decryption tool is a difficult and often expensive decision.

In the United States, no federal laws[2] have been enacted specifically to limit the payment of cyber ransoms.[3] However, the U.S. Treasury's Office of Foreign Assets Control (OFAC) has explained that such payments may subject ransomware victims to liability under the Trading With The Enemy Act (TWEA) and/or the International Emergency Economic Powers Act (IEEPA). Generally, those laws prohibit U.S. persons from transacting or

1. "Ransomware attack" means the deployment of malicious software for the purpose of demanding payment in exchange for restoring critical access to, or the critical functionality of, an information and communications system or network.

2. Some state laws restrict the ability of certain organizations to pay cyber ransoms. *See, e.g.*, FLA. STAT. 282 § 3186(2022).

3. The U.S. federal government has imposed rules for certain organizations, primarily those dealing with critical infrastructure, to report ransomware payments. In addition, money laundering laws require entities involved in the processing of ransomware payments to file disclosures through Suspicious Activity Reports that are submitted to the U.S. Department of Treasury's Financial Crimes Enforcement Network.

attempting to transact with an enemy of the U.S., certain related parties, and specified parties subject to U.S. sanctions or embargoes.

OFAC has published two advisories in recent years on the subject of ransomware payments, both of which suggest that U.S. persons may be held strictly liable under TWEA and IEEPA when they make a ransomware payment to a sanctioned person or engage with an embargoed country or region.[4] Strict liability in this context means that any U.S. person may face a civil enforcement action by OFAC for transacting or attempting to transact with an enemy of the U.S. even if the person did not know or have reason to know that a ransomware payment was being made to a sanctioned person or embargoed country or region.[5]

Contrary to OFAC's advisories, TWEA and IEEPA and their regulations do not impose a strict-liability standard in all cases where a victim makes a ransomware payment to a threat actor on the Specially Designated Nationals and Blocked Persons list ("SDN List"). However, OFAC's interpretation of these statutes and regulations as imposing a strict-liability regime creates substantial uncertainty and unnecessary chilling effects when victims are forced to make ransomware payments. It is often difficult to identify the recipient of a ransomware payment before making it, leaving ransomware victims uncertain about whether

4. *See* U.S. DEP'T OF TREASURY, ADVISORY ON POTENTIAL SANCTIONS RISKS FOR FACILITATING RANSOMWARE PAYMENTS (Oct. 1, 2020), *available at* https://ofac.treasury.gov/media/48301/download?inline [hereinafter OFAC 2020 GUIDELINES] and UPDATED ADVISORY ON POTENTIAL SANCTIONS RISKS FOR FACILITATING RANSOMWARE PAYMENTS (Sept. 21, 2021), *available at* https://ofac.treasury.gov/media/912981/download?inline [hereinafter OFAC 2021 GUIDELINES].

5. Willful or intentional violations of TWEA, IEEPA, or the associated regulations may also result in criminal enforcement by the U.S. Department of Justice.

payment is to a sanctioned person or an embargoed country or region. Additionally, given the federated nature of threat actors and how threat actors align with larger threat groups, it may be very difficult to determine if a payment will be received by a threat actor or group that contains a sanctioned person. Finally, in many scenarios—like those involving risk of physical harm or large-scale economic disruptions—making a ransomware payment could prevent substantial harm. When factors weigh in favor of making the ransomware payment, imposing strict liability is both bad policy and bad law for a ransomware victim, who has no reason to know (and importantly, no time to determine) that the recipient is a sanctioned person or in an embargoed country or region.

This *Commentary* reviews these issues in three parts:

Part 1

An analysis of TWEA and IEEPA; OFAC's recent guidance; and the purported strict-liability standard;

Part 2

A Framework for assisting organizations in identifying the source of an attack and likely recipient of a ransom and evaluating organizations' level of risk from OFAC if the organizations elect to pay; and

Part 3

Suggestions for a more reasoned basis for determining circumstances under which a ransomware payment might be made without the threat of OFAC sanctions.

II. CURRENT LEGAL FRAMEWORK

A. Background

TWEA and IEEPA generally prohibit U.S. persons from transacting or attempting to transact with an enemy of the U.S., certain related parties, and any person, country, or region that is subject to a U.S. sanctions order or embargo ("Sanctioned Parties"). OFAC is responsible for civil enforcement of these laws, issuing related regulations, and maintaining the SDN List, which identifies Sanctioned Parties. According to OFAC, it "administers and enforces [these] economic sanctions programs primarily against countries and groups of individuals, such as terrorists and narcotics traffickers. The sanctions can be either comprehensive or selective, using the blocking of assets and trade restrictions to accomplish foreign policy and national security goals."

Currently, there is no OFAC sanctions program that applies to all ransomware threat actors. Instead, the relevant sanctions primarily affect specific actors who are connected to sanctioned or embargoed nation-states (for example, Evil Corp and Lazarus, which are connected to Russia and North Korea, respectively) and, more recently, certain exchanges for cryptocurrency that have been used by ransomware threat actors to transfer funds. For example, on the SDN List, OFAC has designated the names of individuals known to be affiliated with a particular threat actor (such as Evil Corp) or the name given to their malware (such as Dridex or TrikBot). OFAC has also identified digital wallet addresses used by certain threat actors.

In other words, OFAC's approach to designating threat actors relies on the identity of the Sanctioned Parties. Thus, to determine whether a threat actor is a Sanctioned Party, a ransomware victim must attempt to attribute the attack to an identifiable person or group.

However, as ransomware schemes have proliferated in recent years, and with more attention being paid to sanctioned-party risks, ransomware victims, incident responders, and their legal counsel have faced increasing challenges in trying to determine whether a threat actor is a Sanctioned Party or is affiliated with a Sanctioned Party—a process commonly known as "attribution." Attribution is particularly difficult in the context of cybersecurity threat actors who engage in criminal activity, sometimes act on behalf of (or with the tacit approval of) nation-states; license malware from criminal developers; and generally take extensive measures to obfuscate their identities and activities. Attribution may also take longer than the time allowed by a threat actor for a ransomware payment—i.e., even when the cybersecurity threat actor may be identified, such identification may occur months or years after the immediate incident or the deadline for a ransomware demand.

B. Current OFAC Guidance

There is no published case law that directly addresses OFAC sanctions or enforcement in the ransomware context.[6] OFAC has issued two advisories focused on ransomware[7] (in 2020 and 2021), but those advisories provide little guidance on identifying Sanctioned Parties. Ransomware victims (and the various third parties involved in responding to ransomware incidents)

---

6. In similar contexts involving extortion by Sanctioned Parties, enforcement actions have been brought against parties making payments to the extortionists. *See, e.g.*, Press Release, U.S. Dep't of Justice, Chiquita Brands International Pleads Guilty to Making Payments to a Designated Terrorist Organization And Agrees to Pay $25 Million Fine (Mar. 19, 2007), *available at* https://www.justice.gov/archive/opa/pr/2007/March/07_nsd_161.html#:~:text=Chiquita%27s%20Payments%20to%20the%20AUC&text=Chiquita%2C%20through%20Banadex%2C%20paid%20the,a%20senior%20executive%20of%20Banadex.

7. *See* OFAC 2020 Guidelines and OFAC 2021 Guidelines, *supra* note 4.

therefore face significant uncertainty in trying to determine whether a threat actor is a Sanctioned Party and, in turn, whether a ransomware payment (or their facilitation of such a payment) might be unlawful.

The OFAC advisories identify the risk that ransomware victims and incident responders face from the potential application of a strict-liability standard. Specifically, both advisories[8] explain:

> OFAC may impose civil penalties[9] 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.

In addition, OFAC's Economic Sanctions Enforcement Guidelines[10] identify knowledge and intent factors that will be considered in determining the proper enforcement mechanism in a given case, suggesting that those factors may be relevant only after a liability determination has been made rather than in the liability determination itself.

Nonetheless, to date, there are no reported instances of OFAC bringing an enforcement action against a victim or third party for facilitating a ransomware payment. And OFAC has

---

8. *Id*.

9. The maximum civil penalty amount is adjusted for information by OFAC from time to time. In 2021, the maximum civil penalty amount was the greater of $311,562 or twice the amount of the prohibited transaction. Inflation Adjustment of Civil Monetary Penalties, 86 Fed. Reg. 14,534 (Mar. 17, 2021), *available at* www.federalregister.gov/documents/2021/03/17/2021-05506/inflation-adjustment-of-civil-monetary-penalties.

10. 31 C.F.R. Part 501, App'x A.

not provided any additional clarity regarding its two ransomware advisories. There are, for instance, no FAQs that address issues and questions relating to those advisories, in contrast to the FAQs published by OFAC relating to sanctions against Russia, Iran, and North Korea.[11]

C. When Does Strict Liability Apply?

Despite OFAC's recent advisories and its enforcement guidelines, at least some of the provisions and associated regulations of TWEA and IEEPA do not impose strict liability. For example, multiple provisions of TWEA only prohibit conduct undertaken with "knowledge or reasonable cause to believe" that a counterparty is a foreign enemy or is acting on behalf of such an enemy.[12] Likewise, although certain regulations under IEEPA may impose strict liability,[13] at least some of its provisions and regulations require knowledge or willfulness to establish liability.[14] Ransomware victims and incident responders should therefore be aware that strict liability does not apply in

---

11. *See, e.g.*, *Ukraine -/Russia-related Sanctions*, U.S. DEP'T OF TREASURY - OFFICE OF FOREIGN ASSETS CONTROL, https://ofac.treasury.gov/faqs/topic/1576 (last accessed Oct. 16, 2024).

12. *See, e.g.*, 50 U.S.C. § 4303(a)-(b).

13. *See, e.g.*, 31 C.F.R. § 510.201(a)(1) ("All property and interests in property that are in the United States, that come within the United States, or that are or come within the possession or control of any U.S. person of the Government of North Korea or the Workers'' Party of Korea are blocked and may not be transferred, paid, exported, withdrawn, or otherwise dealt in.").

14. *See, e.g.*, 50 U.S.C. §§ 1705(c) (requiring willful violation to establish criminal liability), 1708(b)(2) (limiting application of section to foreign persons that the President determines "knowingly" engages in subject conduct), 1708(b)(4) (incorporating penalties from section 1705, including criminal penalties for "willful" violations), and 1708(d)(4) (defining "knowingly" for purposes of section addressing economic or industrial espionage in cyberspace).

all cases where a ransomware payment is made to a Sanctioned Party.

1. Legal Standards under TWEA

TWEA makes it unlawful:

> (a) For any person in the United States, except with the license of the President . . . to trade, or attempt to trade, either directly or indirectly, with, to, or from, or for, or on account of, or on behalf of, or for the benefit of, any other person, ***with knowledge or reasonable cause to believe*** that such other person is an enemy or ally of enemy, or is conducting or taking part in such trade, directly or indirectly, for, or on account of, or on behalf of, or for the benefit of, an enemy or ally of enemy.
>
> (b) For any person, except with the license of the President, to transport or attempt to transport into or from the United States, or for any owner, master, or other person in charge of a vessel of American registry to transport or attempt to transport from any place to any other place, any subject or citizen of an enemy or ally of enemy nation, ***with knowledge or reasonable cause to believe*** that the person transported or attempted to be transported is such subject or citizen.
>
> (c) For any person (other than a person in the service of the United States Government or of the Government of any nation, except that of an enemy or ally of enemy nation, and other than such persons or classes of persons as may be exempted hereunder by the President or by such person as he may direct), to send, or take out of, or bring into, or attempt to send, or take out of, or bring

> into the United States, any letter or other writing or tangible form of communication, except in the regular course of the mail; and it shall be unlawful for any person to send, take, or transmit, or attempt to send, take, or transmit out of the United States, any letter or other writing, book, map, plan, or other paper, picture, or any telegram, cablegram, or wireless message, or other form of communication ***intended for or to be delivered, directly or indirectly, to an enemy or ally of enemy***: Provided, however, That any person may send, take, or transmit out of the United States anything herein forbidden if he shall first submit the same to the President, or to such officer as the President may direct, and shall obtain the license or consent of the President, under such rules and regulations, and with such exemptions, as shall be prescribed by the President.[15]

In other contexts, similar legal standards have been construed to impose liability only when a person has actual knowledge of the relevant facts or acts in "deliberate ignorance" or "reckless disregard" of those facts.[16]

---

15. 50 U.S.C. § 4303(a)-(c) (emphasis added). Arguably, 50 U.S.C. § 4303(c) prohibits the cross-border communication of ***any*** "letter or other writing or tangible form of communication" in any other way than "in the regular course of mail," regardless of intent or knowledge as to the source or recipient of the communication. *See* Welsh v. U.S., 267 F. 819, 821 (2d Cir. 1920) (explaining that § 4303 creates two offenses, the first of which does not require any intent that the cross-border communication come from or be directed to a foreign enemy). That section, however, does not appear to have been enforced since the 1920s; it would seem to prohibit significant swaths of modern international commerce, and it might well be unconstitutional.

16. *See, e.g.*, 13 C.F.R. § 142.6 (in the context of Small Business Administration loans, a person knows or has reason to know that a claim or statement

2. Legal Standards under IEEPA

Separately, the penalty provision of IEEPA makes it "unlawful for a person to violate, attempt to violate, conspire to violate, or cause a violation of any license, order, regulation, or prohibition issued under [50 U.S.C. §§ 1701-1708]" and authorizes imposition of civil penalties for any such unlawful act.[17] Standing alone, that provision does not specify the level of knowledge or intent (if any) that must be shown before civil liability may be imposed but instead leaves that question to the language of the particular license, order, regulation, or prohibition at issue.[18] And many of the licenses, orders, regulations, and orders issued pursuant to IEEPA appear to impose strict liability in the sense that they do not have a specific mens rea or scienter requirement.[19] However, the specific provision of IEEPA relating to "economic or industrial espionage in cyberspace" only applies to conduct involving a foreign person "the President determines ***knowingly*** requests, engages in, supports, facilitates, or benefits from the significant appropriation, through economic or

---

is false if the person: "(i) Has actual knowledge that the claim or statement is false, fictitious, or fraudulent; or (ii) Acts in deliberate ignorance of the truth or falsity of the claim or statement; or (iii) Acts in reckless disregard of the truth or falsity of the claim or statement."); *see also* U.S. v. Heredia, 483 F.3d 913, 918, n.4 (9th Cir. 2007) (en banc) ("As our cases have recognized, deliberate ignorance, otherwise known as willful blindness, is categorically different from negligence or recklessness . . . . A willfully blind defendant is one who took deliberate actions to avoid confirming suspicions of criminality. A reckless defendant is one who merely knew of a substantial and unjustifiable risk that his conduct was criminal; a negligent defendant is one who should have had similar suspicions but, in fact, did not.").

17. *See* 50 U.S.C. § 1705(a).

18. *See In re* Criminal Complaint, Case No. 22-mj-067-ZMF, 2022 WL 1573361, at *2 (D.D.C. May 13, 2022) (Faruqui, M.J., mem. op.) (explaining that civil penalties may be imposed under IEEPA "on a strict liability basis").

19. *See, e.g.*, Exec. Order No. 14,065, 87 Fed. Reg. 10,293-96 (Feb. 21, 2022).

industrial espionage in cyberspace, of technologies or proprietary information developed by United States persons."[20]

Moreover, the licenses, regulations, orders, and prohibitions issued pursuant to IEEPA do not, in the aggregate, necessarily prohibit every possible transaction with every person or entity on the SDN List. Instead, those licenses, regulations, orders, and prohibitions are typically issued in connection with a specific conflict, series of events, or set of circumstances relating to a particular country, region, or group.[21] As a result, certain transactions with certain persons or entities on the SDN List would not violate any license, order, regulation, or prohibition issued under IEEPA and thus could not be penalized under 50 U.S.C.

---

20. 50 U.S.C. § 1708(b)(2) (emphasis added); *see also id.* § 1708(d)(4) ("The term ''knowingly,'' with respect to conduct, a circumstance, or a result, means that a person has actual knowledge, or should have known, of the conduct, the circumstance, or the result.").

21. For example, Executive Order 14,065 (recently issued in connection with the Ukraine-Russia conflict) prohibits, among other things:

- new investment in the so-called Donetsk People's Republic [DNR] or Luhansk People's Republic [LNR] regions of Ukraine or [other "Covered Regions"] by a United States person, wherever located;
- the importation into the United States, directly or indirectly, of any goods, services, or technology from the Covered Regions;
- the exportation, re-exportation, sale, or supply, directly or indirectly, from the United States, or by a United States person, wherever located, of any goods, services, or technology to the Covered Regions; and
- any approval, financing, facilitation, or guarantee by a United States person, wherever located, of a transaction by a foreign person where the transaction by that foreign person would be prohibited by this section if performed by a United States person or within the United States.

See Exec. Order No. 14,065, *supra* note 19; *see also* 31 C.F.R. §§ 501-598 and Appendix.

§ 1705(a). Instead, these transactions could be penalized (if at all) only under TWEA, which, as discussed above, by its own express terms does not impose strict liability.

Further, several regulations issued under IEEPA include affirmative defenses or safe harbors relating to the knowledge or intent of the alleged violator.[22] For example, a transfer that would otherwise violate OFAC's Cyber-Related Sanctions Regulations will not be deemed null and void if the alleged violator establishes "to the satisfaction of OFAC" each of the following:

1. Such transfer did not represent a ***willful*** violation of the provisions of this part by the person with whom such property is or was held or maintained (and as to such person only);
2. The person with whom such property is or was held or maintained did not have ***reasonable cause to know or suspect***, in view of all the facts and circumstances known or available to such person, that such transfer required a license or authorization issued pursuant to this part and was not so licensed or authorized . . . ; and
3. The person with whom such property is or was held or maintained filed with OFAC a report setting forth in full the circumstances relating to such transfer promptly upon discovery that:
    i. Such transfer was in violation of the provisions of this part or any regulation, ruling, instruction, license, or other directive or authorization issued pursuant to this part;
    ii. Such transfer was not licensed or authorized by OFAC; or

22. *See, e.g.*, 31 C.F.R. §§ 578.202(d), 589.210(d).

iii. If a license did purport to cover the transfer, such license had been obtained by misrepresentation of a third party or withholding of material facts or was otherwise fraudulently obtained.[23]

In addition, some regulations issued under IEEPA negate strict liability by the language of the prohibition itself.[24]

3. Strict Liability Does Not Apply to All Ransomware Payments to Sanctioned Parties

In light of the foregoing, OFAC's advisories and enforcement guidelines—suggesting that any transaction of any kind with any actor on the SDN List automatically gives rise to strict liability—do not comport with the nuanced text of TWEA, IEEPA, and the associated regulations.[25] Some such payments create strict liability for penalties under IEEPA, but only where they violate a license, order, regulation, or prohibition issued under IEEPA that itself imposes strict liability. Otherwise, such transactions create no strict liability for penalties under either TWEA or IEEPA.

---

23. 31 C.F.R. § 578.202(d) (emphasis added). However, the filing of a report under 31 C.F.R. § 578.202(d)(3) "shall not be deemed evidence that the terms of paragraphs (d)(1) and (2) of [that] section have been satisfied." *Id.* § 578.202(e).

24. *See* Epsilon Elecs., Inc. v. U.S. Dep't of the Treasury, Office of Foreign Assets Control, 857 F.3d 913 (D.C. Cir. 2017) (explaining that 31 C.F.R. § 560.204—which prohibits, among other things, the exportation of goods to a third country that the exporter knows or has "reason to know" are specifically intended for re-exportation to Iran—does not include a strict-liability standard, and OFAC did not argue otherwise).

25. Arguably, OFAC's advisories are accurate to the extent they only reflect that OFAC ***may*** be able to impose strict liability in some cases. Many ransomware victims and incident responders, however, have construed the advisories to mean that OFAC believes strict liability applies in all cases involving ransomware payments to a threat actor on the SDN List.

Courts may give deference to OFAC's interpretation of its own regulations, including potential deference to the statements regarding strict liability in its ransomware advisories.[26] But OFAC's advisories and enforcement guidelines interpret TWEA and IEEPA themselves, and those interpretations should receive no deference.[27]

Accordingly, in attempting to assess the risks and lawfulness of a potential ransomware payment, ransomware victims and incident responders should be aware that strict liability does not always apply.

D. Is OFAC's Licensing Option Feasible in the Ransomware Context?

OFAC has a licensing process that theoretically could be used in the ransomware context and that OFAC suggests is an option in its advisories. OFAC offers two types of licenses: general and specific. General licenses are not specific to the applicant but, instead, authorize a particular type of transaction for a class of persons without the need to apply for a specific license. There are no general licenses that currently apply to ransomware payments.

A specific license is a written document issued by OFAC to a particular person or entity authorizing a transaction in

---

26. *See* Kisor v. Wilkie, 588 U.S. 558, 576 (2019) (even nonbinding interpretations of agency's own regulations may be given deference under *Auer v. Robbins*, 519 U.S. 452 (1997)).

27. *See* Loper Bright Enterprises v. Raimondo, 603 U.S. —, 144 S.Ct. 2244 (2024) (*overruling* Chevron, U.S.A., Inc. v. Nat. Res. Def. Council, Inc., 467 U.S. 837 (1984)); *see also* Christensen v. Harris Cty., 529 U.S. 576, 587 (2000) (unlike an agency's interpretations of its own regulations, its informal interpretations of statutes, "like [those] contained in policy statements, agency manuals, and enforcement guidelines, all of which lack the force of law" did not receive deference even under *Chevron*).

response to a license application. The specific license application process involves an application that can be submitted on OFAC's website. Typically, a license applicant should include as much detail about a transaction as possible, including the purpose of the license, the names and contact information of all parties involved, and as much documentation as possible.

There is no timeline for OFAC to issue a decision on a license request. OFAC warns that the length of time will vary depending on the complexity of the transaction(s) under consideration, the scope and detail of interagency coordination, and the volume of similar applications awaiting consideration. From collected prior experience, it may take OFAC several months to several years to respond to license requests (with simpler transactions on the lower end, which a ransomware payment is not). OFAC grants specific licenses on a case-by-case basis but noted in its September 2021 Advisory that OFAC will apply a presumption against granting specific licenses in the ransomware context.[28] Technically, it is possible to appeal a denial of a specific license as a "final agency action" in federal court under the Administrative Procedure Act. It is unlikely, however, that such an appeal will be successful given the current deference afforded OFAC by courts.

Practically speaking, victims and incident responders trying to use the licensing process in the ransomware payment context face major hurdles. First, the victim must know the ransomware payment is going to an individual SDN or otherwise implicates a sanctioned country, region, or government, but strong attribution to an SDN or sanctioned region in the beginning of a ransomware incident is difficult for the reasons described above. Certainly, the ransomware victim could submit an online application without providing much information. But there is no

28. OFAC 2021 Guidelines, *supra* note 4.

reason to ask for a license from OFAC if the ransomware victim does not know the transaction is prohibited by OFAC. Similarly, OFAC will not grant a specific license if the underlying transaction is not prohibited—in those situations, OFAC may provide a No License Required determination, which in itself can act as assurance that the conduct for which a license was sought does not fall within the category of prohibited activity. Therefore, submitting a license application without sufficient information is not likely to result in anything more than alerting OFAC of the issue before making a payment (which is not the purpose of seeking a specific license).

Second, assuming the ransomware victim has the information sufficient to complete the application, the victim needs to file an application for a specific license and receive a response from OFAC—granting the license—before making a payment. Most ransomware victims, however, are not in a position to wait months or years for OFAC's decision before making a payment; the act of delaying the payment pending a decision by OFAC on a license instead may function as a decision not to make the payment at all (especially given potential ransomware demand deadlines).

Third, and most compelling, OFAC has said there is a presumption against granting a license in the ransomware context. This presumption is a strong indication that OFAC is not willing to use the license process to resolve the sanctions issue faced by victims who decide they need to make a ransomware payment. It also means that a victim seeking an OFAC license may delay or decline to make a ransomware payment pending the outcome of OFAC's determination, only to have that license denied and the victim end up in the same situation it started with—forced to decide whether to make a ransomware payment without any understanding as to whether it's prohibited by OFAC or could subject itself to liability.

Absent a Freedom of Information Act request, there are no publicly available statistics tracking license applications, but the drafters' collective experience suggests that there have been very few, if any, licenses granted in connection with ransomware payments. For example, some insurers have sought licenses to reimburse ransomware victims, but it appears that no such licenses have been granted.[29]

In sum, due to the accelerated speed needed for a payment decision, the slow speed of the OFAC licensing process, and OFAC's reluctance to weigh in on attribution, the current license process is not a workable solution for ransomware victims, incident responders, or legal counsel concerned about OFAC enforcement.

E. OFAC's Approach Generates Uncertainty and a Chilling Effect

Despite scant enforcement activity in the ransomware context, OFAC's guidance and lack of a viable licensing option have affected incident responders in several ways:

- Most incident response companies have instituted some type of OFAC compliance check process, starting with rudimentary checks of digital wallets against the SDN List (a largely feckless process given that most threat actors create and dispose of wallets for each attack). Many of the OFAC compliance checks completed by incident responders or a ransomware victim's counsel rely on unreliable and unverifiable technical indicators, which are often

29. This is perhaps a scenario in which a license involving ransomware might make sense or would at least be feasible—i.e., a situation in which cyber insurance coverage may be available to a ransomware victim, but an SDN has been identified as the payee after the victim has already made the payment but before the insurer has reimbursed the victim.

difficult to assess precisely because threat actors obfuscate to avoid law enforcement and being placed on a no-pay list (if they were identified with an SDN/sanctioned country).

- Certain ransomware threat actors have been placed on no-pay lists by some incident responders for reasons related to OFAC's advisories. For example, some companies stopped payments to the Russian threat actor Conti when some reports linked its operators to Russian security services. In another instance, a threat actor advertised that it was shifting its hosting services to Iran, which immediately led to at least one incident response company banning payments to that threat actor. In response, the threat actor promptly issued a second press release walking back its plan to shift to Iran.
- The professionalization of ransomware-as-a-service (RaaS) platforms has further complicated the attribution for OFAC purposes. RaaS allows a segmentation of the cyberattack process. Broadly speaking, threat actors have specialized for-sale services for each of the four phases of a ransomware attack—access, network mapping, malware deployment, and ransomware detonation. This makes "attribution" that much more difficult given that different groups play different roles in different aspects of a ransomware attack.
- As part of the OFAC check, some incident response companies go so far as to ask the threat actors, during the payment negotiations, to identify themselves.

- Anecdotally, we also understand that some ransomware victims and incident responders prefer not to ask which threat actor is involved, under the mistaken theory that ignorance presents some defense or makes it more likely that cyber insurance will not be put at risk.
- Almost all insurance carriers offering cybersecurity coverage require some form of "sanctions" attestation before authorizing ransomware payments under a policy.[30]

Further, under OFAC's guidance, the implications for incident responders appear clear on the surface but are in fact problematic. On the one hand, the OFAC advisories appear to suggest that all entities involved in incident response—from legal counsel and forensic investigators to companies facilitating the transfer of cryptocurrency—can mitigate the risk from an unintentional dealing with an SDN or a threat actor in a sanctioned country. In theory, this can be done by instituting compliance checks and working with law enforcement. This is difficult to accomplish in reality for two reasons. First, most of the information likely to assist incident responders with attribution is in the hands of either the government (FBI, Secret Service) or some of the largest cybersecurity companies. Second, organizations must make a payment decision in an accelerated time frame that leaves very little time to determine the identity of a threat actor who is committed and has taken specific steps to mask its identity. This leaves OFAC's suggestions for mitigation without any practical means for implementation during an actual incident. More specifically, incident responders are left to rely upon their own experience with past clients, open-source/public reporting,

30. These attestations would likely do little to protect the carriers if OFAC applied a strict liability approach.

or, in limited instances, whatever information is available from law enforcement.

This haphazard approach incident responders are forced to undertake to identify a threat actor is in stark contrast to the kind of processes that businesses in the U.S. have implemented to comply with other OFAC requirements—e.g., collecting know-your-customer ("KYC") information on banking customers or registration/ownership documents for third parties, which can then be screened against the OFAC SDN List.[31]

A similar compliance approach to OFAC checks for ransomware is very difficult with respect to threat actors that operate in criminal forums and are often highly motivated and skilled in obfuscating their nationality or location. Moreover, OFAC itself provides no actionable information on how to identify an SDN in the ransomware context. Again, some of OFAC's ransomware-related designations involve identifying certain digital wallets associated with a handful of threat actors, but as noted above, such identification is largely meaningless, given the disposable nature of those wallets. And, to the extent that OFAC has designated a ransomware "group" by a moniker such as "Evil Corp," or by reference to a type of ransomware, such as Dridex, that is unhelpful because these groups are informal, constituted ad hoc, and often use specialists who may work across several groups or platforms.

In short, ransomware incident responders can rarely be sure whether a threat actor is a Sanctioned Party; thus, they can rarely be sure whether a ransomware payment is lawful. As a result, many ransomware victims may choose not to make ransomware payments, even when doing so would have been

31. Despite being well established and generally effective, these KYC processes still fail frequently—due, for example, to incorrect spellings of names or other technical or human errors—and such failures can still lead to liability.

lawful (where the threat actors are not, in fact, Sanctioned Parties), and perhaps even when doing so would prevent substantial economic hardship and/or physical harm.

III. ASSESSING THE RISK OF MAKING A RANSOMWARE PAYMENT

A. Introduction

Regardless of whether strict liability or some other standard (such as "knowledge or reasonable cause to believe") applies, organizations plainly face some level of sanctions-related risks in making ransomware payments. This section provides guidance on appropriate steps to assist in the attribution process and a discussion as to how the findings from that process, even if inconclusive, can inform the level of sanctions-related risk if a payment were to be made.

B. Attribution Process

The process of attributing the activities surrounding a ransomware attack to a given threat actor or crime syndicate is more art than science. The process outlined below cannot provide certainty that the hands on the keyboard are the threat actor; however, it provides a Framework for ransomware victims to evaluate risk.

The ransom note is the first line of identification. Threat actor notes are customized to their brand. For example, the ransom note created by Hive ransomware states that it is from the Hive threat actor group and provides information on a Tor Node with the group's leak site and a channel for communications. These notes are cataloged on many third-party sites and by law enforcement. Lastly, most threat actors have a leak site, maintained in the deep and dark web, where ransomware victims are directed.

After the ransom note has been provided, secondary indicators are used to complement the analysis. These indicators can include forensic findings such as the 1) encryptor used, 2) the internet protocol (IP) addresses used by the threat actor, 3) the attack kit, such as scanning tools, used by the threat actor, 4) the

manner in which data exfiltration was performed by the threat actor (if applicable), and 5) discussions with third-party sources such as law enforcement regarding any similar such attacks at other organizations.

The encryption tool, if recoverable, provides many clues on the coding of the malware. For example, Alpha Black Cat uses an encryptor built on the RUST platform. The encryption program will normally generate the ransom note after the tool is run during the attack. A properly equipped researcher can run the tool in a safe sandbox environment, which can help to understand the algorithms used and then use that information to connect to certain threat groups. This detailed investigation takes both trial and error, dedicated effort, and most importantly, time.

Once an agreement on payment is made with the threat actor, a cryptocurrency wallet identifier is provided, and that identifier may be another indicator to determine whether a Sanctioned Party appears to be the intended recipient of the funds. Although ransomware incidents typically involve unique, one-time-use wallets created specifically for each attack, some wallets have been tied to certain threat actors through forensic analysis, which can allow for subsequent identification, but usually well after the incident. Wallets can also be examined through several programs that provide intelligence about the wallet being used, the cryptocurrency exchange, and other potentially useful information.

Another approach is to combine sources of information, such as blockchain analysis, detections from the ransomware victim's network systems, and threat intelligence analysis and other research, to provide counsel and client with as much information as possible to make an informed decision as to whether a threat actor is a Sanctioned Party.

As above, blockchain analysis examines the cryptocurrency wallet provided by the threat actor. Cross-checks can be performed against the wallet itself, and any other wallets associated with it, as well as transactions against the wallet, against the Sanctioned Party, and other global watchlists. Various tools can provide insights on the threat actor's wallet, as well as other associated wallet addresses previously seen by the incident response firm. To underscore, these are usually retrospective due-diligence steps with limited utility during an incident where a threat actor uses a fresh wallet.

The ransomware victim's antimalware or endpoint detection and response system will contain indicators of compromise and/or malware signatures that can be compared against government repositories, other threat intelligence sources, or the incident response firm's own database of indicators of compromise. Other evidence will include the behavior of the malware within the environment, such as the method of infiltration and how the malware moved through the ransomware victim's environment, which can be matched against behavior patterns of other variants. Information can sometimes be gleaned from reverse-engineering the malware.

Other sources of intelligence include the incident response firm's security operations center, forensic vendors, and open-source intelligence—the dark web, or information from other security researchers. Cooperation with law enforcement is an important step that should be encouraged and has, on occasion, provided some valuable information.

If and once a payment is made, additional tracing of the wallet is generally not performed by the ransomware victim or incident responder. However, postpayment tracing may be undertaken by law enforcement, the Treasury Department's Financial Crimes Enforcement Network, and certain companies involved in monitoring crypto exchanges, who are building up

more granular tracing information. Another exception is when a threat actor re-ransoms a client for additional funds and provides a new wallet ID to the ransomware victim—in that instance, the original wallet ID would usually be reanalyzed.

C. Framework for Assessing Risk of Payment

The process of attributing a ransomware attack to a threat actor is complex, time-intensive, and has an uncertain outcome. Experienced forensic analysts who have handled hundreds of ransomware attacks may not be able to reliably attribute a ransomware attack to a particular threat actor. In fact, in many cases, a lack of reliable attribution is the assumed result.

The OFAC strict liability structure for payments to Sanctioned Parties thus gives rise to significant uncertainty for companies contemplating whether to make a ransomware payment. To help ransomware victims assess the degree of OFAC risk they may face for making a ransomware payment, this *Commentary* proposes a Framework. Due to the relative opacity of existing OFAC guidance, the lack of any OFAC sanctions to date against entities making payments to Sanctioned Parties, and a lack of judicial rulings, it is not possible to quantify the risk to an entity for making a prohibited payment. The proposed Framework instead serves as a methodology to enable entities to assess a level of risk of liability, as well as enforcement, based on the standards and guidance provided by federal regulatory authorities to date.

1. Framework Overview

The Framework involves consideration of two separate but related legal risks. First, the legal risk that a payment is actually sent to a Sanctioned Party, thus triggering strict liability under the OFAC regime; and second, whether mitigating factors exist to influence the level of OFAC's sanctions if it chooses to enforce

sanctions on an improper payment. There are different facts and variables informing an analysis of each question. The ultimate legal risk to an organization considering whether to make a payment involves consideration and balancing of both risks.

The Framework borrows elements of the risk assessment methodology often used by information security groups when evaluating, for example, the sufficiency of their control environments. The Framework seeks to define "inherent risk"—the risk of OFAC liability based on attribution efforts—and "residual risk," which is the bottom-line risk to an entity when considering inherent risk as well as mitigating factors.

The Framework adopts certain key principles:

- First, although strict liability may not apply in all situations, as described above, the Framework assumes that OFAC would likely seek to impose strict liability in any enforcement action.
- Second, under the strict-liability Framework, the reasonableness of the steps an entity takes to attribute a ransomware attack to a threat actor would have no bearing on whether a legal violation has occurred. The reasonableness of an organization's prebreach and postbreach actions, however, could be mitigating factors that would reduce the severity of any OFAC enforcement or imposed penalty.[32]

32. OFAC has identified the factors it considers in determining the nature and extent of any enforcement action. *See* 31 CFR Ch. V, pt. 501, App'x A. However, the drafters of this *Commentary* believe OFAC should provide additional clarification regarding its understanding of strict liability in this context and its application of mitigating factors.

- Third, in general, as confidence that a threat actor is a Sanctioned Party increases, inherent legal risk increases.

2. Applying the Framework

Hypothetical One

A large, sophisticated organization suffers a ransomware attack that significantly degrades its ability to timely process new online customer orders. The organization has completed regular employee training, maintains an information security plan that aligns with relevant regulatory and industry standards, and has a robust business continuity plan that is nonetheless unable to fully restore affected servers. The organization files an Internet Crime Complaint Center (IC3) report and remains in regular dialogue with the FBI concerning the event.[33]

The threat actors appear to be a new or unknown group, based on the contents of the ransom note. The organization retains specialized ransomware negotiators to assist in negotiating with the threat actor and assessing whether the threat actor is on the OFAC SDN List. By assessing indications of compromise, forensic analysts believe the malware signature points to one of four possible threat actor groups. The analysts do further blockchain analysis of the crypto wallet that the threat actors provide for facilitation of the ransomware payment. This analysis leads the experts to conclude that there is a significant probability that the threat actors are Iranian nationals.

33. The Internet Crime Complaint Center (IC3) is the FBI's standard portal for reporting cybercrime.

Risk Assessment

Attribution Steps	• Indications of compromise • Ransom note • Blockchain analysis • Threat intelligence
Confidence Level	Significant probability that actors are Iranian nationals
Inherent Risk	High
Mitigation Factors	• Incident Response Plan • Regular training • Business continuity program • Notification to and regular communications with federal authorities
Residual Risk	Medium-High

Analysis

This scenario involves a sophisticated organization that undertakes substantial efforts to attribute a ransomware attack. Those steps reveal a high likelihood that the threat actors are Sanctioned Parties or affiliated with Sanctioned Parties. Therefore, a ransomware payment to the threat actors would be in violation of OFAC sanctions, giving rise to a significant possibility of penalties based on OFAC's stated position.

However, the organization has also undertaken substantial preattack steps to prepare for, avoid, and remediate a ransomware attack. The organization also promptly notified federal authorities about the event and kept them regularly informed. These are mitigating factors that should lessen the likelihood of OFAC enforcement, and the organization could make a voluntary disclosure to OFAC itself, which might further reduce the risk of penalties.

Based on all of the foregoing, the residual legal risk of an OFAC penalty in this instance is medium-high, based on the high inherent risk.

Hypothetical Two

A small university lab suffers a ransomware attack that encrypts its research files, due to a phishing email. The university has not conducted any cybersecurity training for lab employees but uses multifactor authentication on relevant systems, pays for sophisticated antimalware software, and has a large IT department that enacts the university's incident response plan. The IT department is unable to restore the affected files, and the university files an IC3 report and responds in a timely fashion to additional questions from the FBI.

The threat actor identifies itself as a known group in the ransom note and is not on OFAC's SDN List. The university hires a ransomware specialist to further analyze the note and indications of compromise. The specialist finds that the attack is consistent with two other verified attacks by the self-identified threat actor. The specialist also conducts a blockchain analysis of the crypto wallet, which has been previously used, and concludes with a high degree of confidence that the wallet has been previously used by a threat actor not on the OFAC SDN List.

Risk Assessment

Attribution Steps	• Indications of compromise • Ransom note • Blockchain analysis • Threat intelligence
Confidence Level	High degree of confidence that actors are not on the SDN List
Inherent Risk	Low

Mitigation Factors	• Basic cyber hygiene practices • Incident Response Plan • Notification to and regular communications with federal authorities
Residual Risk	Low

Analysis

The ransomware victim is a small university lab that could have taken more preattack cyber hygiene steps to prevent the ransomware attack, such as regular employee training. Universities are an increasingly common target of ransomware attacks. However, the lab responds appropriately once the attack is made, and its attribution efforts reveal a low likelihood that the threat actors are on the OFAC SDN List. Therefore, a ransomware payment to the threat actors is unlikely to violate U.S. law or trigger any OFAC enforcement action.

Hypothetical Three

A medium-sized software development organization is the victim of a ransomware attack that results in the exfiltration of sensitive data and subsequent encryption of local file shares containing valuable customer data. The file shares had not been backed up.

Prior to the ransomware attack, the organization was in the process of building out its cybersecurity program but had been hampered by cost concerns and the recent departures of key employees from the Information Security department. The organization had not done cybersecurity training for employees in several years. In fact, the organization was surprised to learn that the data was even stored on local file shares, as its policies required storage of customer data in a secure cloud environment.

In response to the ransomware attack, the organization filed an IC3 report and reached out to local FBI agents, who provided

limited support and did not express significant interest in the attack. The organization also retained a forensic consultant. The consultant examined indications of compromise and other forensic artifacts, including the ransom note, and judged it more likely than not that the malware was not associated with any known threat actor groups, including any groups on the OFAC SDN List. Due to cost constraints, the organization declined to perform a blockchain analysis. The organization arranged payment to the threat actors and filed a Suspicious Activity Report (SAR) with the U.S. Treasury Department.

Risk Assessment

Attribution Steps	• Indications of compromise • Ransom note
Confidence Level	Moderate confidence that threat actors are not on SDN List, but this is based on truncated forensic analysis
Inherent Risk	Medium
Mitigation Factors	• Some cyber policies; immature cyber program • Violation of internal storage policies • IC3 report • FBI contact
Residual Risk	Medium

Analysis

This hypothetical involves incomplete attribution efforts that are arguably justified by virtue of the significant danger to the organization's business if a payment were not made to the threat actors, given the lack of backups. While there is no clear indication that the threat actors are on the SDN List, the organization could arguably have done more to confirm this assessment. The organization's prebreach mitigation efforts are,

likewise, less than complete. The organization's cyber program was immature, employee training was out of date, and there was a clear policy violation that led to the improper storage of customer files on local file shares that were not backed up. Post-breach mitigation efforts include filing of an IC3 report, outreach to the FBI (whose lack of interest may itself have been an indication that the threat actors were unlikely to have been on the SDN List), and the filing of an SAR. Overall risk in this scenario is medium, largely due to the lack of any forensic evidence of attribution to an entity on the SDN List and the FBI's apparent lack of concern. The overall risk, however, is not low because the organization's mitigation efforts were poor, and its attribution efforts could have gone further.

Hypothetical Four

A small dentist's office suffers a ransomware attack through a phishing campaign that affects access to a small volume of highly sensitive data: the Social Security numbers, financial information, and names of patients. The office previously conducted regular employee trainings on cyber hygiene but has not conducted any training since a change in management five years ago. The office uses antivirus software and believed that was sufficient to protect against cyberattacks. Employees searched for an incident response plan or policy but could not find one in the office's files. The office never renewed the cyber insurance policy that it carried up to five years ago prior to the management change, and no one at the office understands that an IC3 report should be filed. Several public postings have identified this threat actor as based in North Korea, based on a unique ransom note. The threat actor also identified itself as a North Korean group. The office pays the small ransom demand without consulting outside experts in an effort to avoid disruption to the practice and avoid giving notice to patients of the breach.

Risk Assessment

Attribution Steps	• Indications of compromise • Ransom note
Confidence Level	High probability that actors are North Korean nationals
Inherent Risk	High
Mitigation Factors	None
Residual Risk	High

Analysis

This scenario involves an unsophisticated business that undertakes no effort to attribute the ransomware attack or determine the legality of payment. The ransom note itself reveals a high likelihood that the threat actors are on the SDN List, although 100 percent attribution is not possible from a ransom note alone, given that threat actors are in the practice of obfuscation and deceit. Here, the ransomware payment to the threat actor is a clear violation of OFAC sanctions, giving rise to a significant possibility of penalties based on OFAC's stated position.

The business has undertaken minimal and outdated cyber hygiene steps and no postbreach mitigating actions, such as contacting law enforcement. In deciding not to consult an outside expert, office employees may have operated under the mistaken theory that ignorance would shield them from liability. The failure to notify patients of the breach presents additional risks beyond OFAC enforcement, including legal risks under state and federal data-protection and breach-notification laws.

The residual legal risk of an OFAC penalty in this instance is high, based on the high inherent risk, deliberate ignorance, and absence of mitigating factors.

IV. A PROPOSAL TO ADVANCE THE LAW: CREATION OF A SAFE HARBOR

A. Background

It is in the best interest of public policy that illegal and/or unauthorized cyber intrusions of all manner, scope, and scale are minimized or eradicated if possible. Paying ransoms to cyber threat actors is not a desirable outcome. OFAC summarized the situation thusly: "Such payments not only encourage and enrich malicious actors, but also perpetuate and incentivize additional attacks."[34]

That, however, is not the full extent of the story. This *Commentary* raises the question of whether preventing ransomware payments, based solely upon the presumed identity of the recipient of the funds, is a good or useful public policy. Arguments in favor of the public policy include: (a) fewer ransomware payments overall are likely to be made, based upon both prohibition when attribution can be made and the uncertainty generated when it cannot; (b) the most harmful nation-states and criminals, listed as Sanctioned Parties, should overall receive reduced funds from their criminal activities; and (c) with the reduced likelihood of ransomware payments, threat actors will be disincentivized from pursuing such activities.

Arguments against such a policy include, most prominently, the difficulty in determining the recipient of the funds, especially in the short timeframes necessary in ransomware scenarios. Section II(e), above, describes this difficulty in detail along with some of its consequences, including: (a) a chilling effect on advisors when they are most needed; (b) imposition of punishment for payments to Sanctioned Parties made by mistake; and (c) victims foregoing ransomware payments and incurring

34. OFAC 2021 Guidelines, *supra* note 4.

significant negative consequences on organizations, customers, clients, and other related third parties, even when such payments may have been legal, in the organizations' best interests, or have created significant and beneficial effects for third parties.[35]

In addition, there are situations where the benefits of making a ransomware payment might outweigh the costs and negative effects of paying a Sanctioned Party. For example:

- Healthcare: A hospital able to return to full operational capacity in hours or days, instead of weeks, reduces the risk of physical harm to patients who might not be able to receive proper treatment.
- Government Services: A water treatment or power-generating facility operating without proper safety controls or having to be shut down can endanger thousands of individuals.
- Economic: A large local or regional business that will suffer significant harm could endanger hundreds or thousands of jobs and the local economy.

Current guidance, however, does not specifically include consideration of these attack-specific circumstances. Accordingly, in keeping with The Sedona Conference's mission to move the law forward in a just and reasoned way, this *Commentary* identifies an alternative "safe-harbor" Framework that may offer a better path forward and be worthy of consideration.

---

35. *See, e.g.*, Jane Doe v. Lehigh Valley Health Network Inc., Case # 3:2023cv00585 (M.D. Pa. Apr. 6, 2023). The plaintiffs are patients whose nude healthcare photos were published by threat actors after the defendant refused to pay a ransom. https://dockets.justia.com/docket/pennsylvania/pamdce/3:2023cv00585/137513.

B. A Safe Harbor Framework

A "safe harbor" Framework may balance conflicting concerns. Generally, such a Framework would identify specific legal actions organizations can take to minimize or remove a specific legal liability that would otherwise attach in a given scenario.

In the ransomware payment scenario, this *Commentary* proposes that compliance with certain cybersecurity-related prerequisites could protect an organization from OFAC enforcement or otherwise reduce or eliminate OFAC-related liability for an organization making a ransomware payment to a Sanctioned Party. The discretion afforded to organizations who meet the prerequisites, we hope, would incentivize the voluntary adoption of better cybersecurity practices that immediately increase an organization's cybersecurity posture and, in the longer run, potentially lessen the severity of a cybersecurity attack if one occurred. This proposed safe harbor would not limit or eliminate any other liability in litigation or any federal, state, or administrative/regulatory proceeding. Nor, in the unfortunate event of a successful attack, would organizations that qualify for the safe harbor be required to pay a ransomware payment. It also would not immunize conduct in situations in which organizations know or have reason to know that they are facilitating payments to Sanctioned Parties. Organizations qualifying to make a ransomware payment may still ultimately elect to forego payment for a variety of reasons. In the best scenarios, such organizations will have undertaken sufficient preparation such that they do not obtain a substantial benefit from making a ransomware payment.

To be useful and successful, such a Framework must follow certain basic principles:

Principle 1: Minimum Security Standards. The safe harbor should only be available to organizations that

> **have implemented a minimum baseline of security controls and practices to reduce the overall risks of ransomware attacks and ransomware payments.**

The prerequisites necessary to qualify for the safe harbor can encompass various capabilities, which, if followed, should reduce overall risk and make ransomware attacks and payments less likely. Of course, attack methods and new technologies are constantly evolving, so the mandated controls and processes must be flexible enough to evolve with them. This *Commentary* has considered the sample factors and requirements set forth in Appendix A.

The *Commentary* acknowledges that, ideally, a ransomware safe-harbor qualification would address both the difficulties of attribution and balancing the potential harms to life, liberty, and the economic area or region (i.e., loss of jobs versus potential for facilitating a terrorist attack). Minimum security standards focus on the cyber hygiene of organizations prior to a cyber security attack. Increased cybersecurity posture helps to ensure that organizations are better positioned during the determination phase of attribution.

However, the *Commentary* maintains that minimum-security standards are nonetheless the best qualifier for the safe harbor in the context of ransomware payments. A balancing process is simply not practical. Most ransomware events include the possibility of harm to some individual or organization, and there is no practical method to weigh relative harm. Furthermore, in the compressed timeframe of a ransomware attack, entities may struggle to apply an imprecise, harm-based test. By contrast, as is discussed in greater detail below, it is significantly easier to make a "yes/no" determination of whether certain minimum-security standards have been met. Meanwhile, the upfront

capital costs and efforts that enhance cybersecurity and resilience should be encouraged and rewarded.

Principle 2: Clarity. The controls and practices required to qualify for the safe harbor should be sufficiently clear to permit organizations to quickly determine whether they qualify.

As discussed above, decisions regarding ransomware payments must be made quickly. Thus, for a safe harbor to be beneficial, organizations must be able to quickly determine whether they have qualified (better yet, they should be able to make this determination before an attack, if they have sufficient opportunity).

This means that any requirements must be reasonably specific. Sliding-scale requirements, such as those requiring organizations to adopt controls commensurate with their risk appetite, would reduce the usefulness of the safe harbor by preventing organizations from quickly determining whether they qualify. Therefore, efforts should be made to define the qualification requirements with the greatest specificity possible—perhaps, for instance, through identifying specific (but still adaptable) mandated controls and processes like those described in Appendix A.

The adoption of a preexisting framework, such as an NIST or ISO framework, for the safe harbor was considered but rejected. Such valuable but very detailed frameworks are sufficiently complex that organizations may struggle to determine whether they qualify for the safe harbor, thus defeating its purpose. Preferably, the safe harbor would identify a select number of controls and practices deemed most critical to resilient cybersecurity and identify specific thresholds applicable to organizations depending on their scale. However, a third-party certification of a cybersecurity standard such as ISO 27001 may be considered a superset of the controls required for the safe

harbor. As such, while they should not be required for safe harbor qualification, such certifications might be considered as automatic qualification.

Principle 3: Scaling Flexibility. The controls and practices required to qualify for the safe harbor should scale to account for organizational differences in sophistication, funding, personnel, and other real-world issues that often limit adoption of controls and processes, while setting minimum standards needed to mitigate and prevent as much facilitation of money to Sanctioned Parties as possible.

A safe harbor test should be flexible enough to recognize and account for organizational differences. To address these disparities while also maintaining simplicity and ease of use, easily determined categories—perhaps based upon an average annualized revenue or similar proxy for sophistication and budget capabilities—could be created along with requirements for controls and processes that scale to reflect what might reasonably be expected of organizations in each such category. Such a test should identify those processes that are most likely to assist organizations in preventing the transfer of funds to Sanctioned Parties so as to facilitate OFAC, foreign policy, and national security goals.

Principle 4: Technological Flexibility. The controls and practices required to qualify for the safe harbor should adapt to developments in technology, security, the law, and the threat landscape.

Cyber threats are constantly evolving, forcing the related technologies, security controls, and laws to keep pace (or at least *try* to keep pace). The safe-harbor qualifications, therefore, need to be flexible enough to adapt to changes quickly. Accordingly, to the extent that the safe-harbor qualifications are based upon

some third-party framework (*see* Principle 2: Clarity), it should be made clear that any applicable changes to that third-party framework are presumptively adopted into the safe-harbor qualifications. Similarly, if a regulator (either OFAC or another body) is responsible for creating the qualifications, then that regulator should also be: (1) required to routinely review the qualifications to evaluate whether changes are necessary; and (2) empowered to update the qualifications as quickly as possible.

Principle 5: Prepayment Notification. The safe harbor should require an organization to notify OFAC before making a payment.

Before receiving the benefit of the safe harbor, organizations should also be required to file a prepayment report with OFAC no later than 24 hours[36] before making the ransomware payment. The reporting regimen would be similar to the existing requirements for SARs. Filing a prepayment report would not relieve the payor from complying with any other provision of law.

The prepayment report should include a description of the ransomware attack, the ransomware payment demanded, and all other information concerning the ransomware attack obtained through good-faith efforts, including the party who committed the attack and demanded the payment (if known), and all other identifying information. Information about the ransomware payment should include the identity and verification of the hosted wallet[37] and the person who will engage in

36. A prepayment report should be updated upon any material change in circumstance or knowledge prior to payment being made. However, the update should not restart the 24-hour waiting period.

37. Hosted wallets are those for which a financial institution provides custody services for its customers'' convertible virtual currency.

transactions with unhosted[38] or otherwise covered wallet counterparties.

OFAC encourages victims and those assisting them with ransomware attacks to report the attacks and to contact OFAC if they suspect there may be a sanction connected to the ransomware payment. A safe harbor with a prepayment component would beneficially increase ransomware attack disclosure, providing the government with quick attribution information. Under the current framework, ransomware victims may choose to not report ransomware attacks at all or to delay their reports, rendering the information more remote and less useful.

38. Unhosted wallets are those that store private keys for convertible virtual currency in a software program or written records to conduct transactions privately rather than using the services provided by a financial institution.

V. CONCLUSION

OFAC's advisories and enforcement guidance suggest that a ransomware victim may be strictly liable whenever it makes a ransomware payment to a Sanctioned Party. Such strict liability does not apply in all circumstances, however, as the language of TWEA and IEEPA and the regulations thereunder make clear. OFAC's guidance regarding this issue creates a chilling effect on ransomware payments and may prevent ransomware payments that would be legal and would have positive net benefits. That guidance complicates matters not only for ransomware victims but also their incident responders, legal teams, negotiators, and insurers.

In the absence of further guidance or authority, ransomware victims may wish to utilize the risk-based Framework set forth above in attempting to attribute a ransomware attack and assess the potential liability resulting from a ransomware payment. However, OFAC and related policymakers should consider providing additional guidance and creating a safe harbor to encourage and enhance cybersecurity controls for all organizations.

APPENDIX A – SAMPLE FACTORS AND REQUIREMENTS FOR CONSIDERATION

Factor	Requirements
A. Governance	For all organizations, of any size: i. formal oversight by a qualified individual and/or board oversight; ii. written cybersecurity policies and procedures; iii. written incident response plan; and iv. annual certifications of compliance to a board or appropriate ownership group

Factor	Requirements
B. Technical Safeguards	For all organizations, of any size, multi-factor authentication for network access and email client access, along with password control protocols. The next level might add additional servers, endpoint detection and monitoring, and regular patching protocol. The highest-level organizations could be required to also implement: i. centralized firewall and security logging (with adequate retention period); ii. appropriate and reasonable network segmentation; iii. network and system monitoring; and iv. encryption in transit and at rest of any statutorily defined and protected class of personal information.

Factor	Requirements
C. Risk Assessments	For all organizations, of any size, annual penetration testing. The next level might add requirements to conduct: i. asset inventory; ii. data classification and criticality rating assessment; and iii. vulnerability scanning. The most sophisticated organizations would be required to conduct: i. cloud configuration assessments; ii. network assessments and mapping; and iii. annual vulnerability scanning.
D. Controls	All organizations, of any size, should conduct regular tabletop exercises. More sophisticated organizations should also: i. implement privilege access controls program; ii. ensure timely and effective data disposition; and iii. maintain audit trails and logs of data at rest, data in transit, and data in use.

Factor	Requirements
E. Postincident	All organizations would be required to notify appropriate law enforcement entities and extend cooperation to such law enforcement entities during any investigative process (e.g., sharing indicators of compromise).