

The Sedona Conference WG11 Brainstorming Group Outline – When are ransomware payments illegal under current U.S. law? (April 2022)



**The Sedona Conference
WG11 Brainstorming Group Outline – When are
ransomware payments illegal under current U.S law?
(April 2022)**

Brainstorming Group Members:

Jim Shook (Brainstorming Group Leader)
Carol Alexis Chen
Guillermo Christensen
John Gray
Sandra Taylor
Larry Wescott
Al Saikali (Steering Committee Liaison)

**The Sedona Conference WG11
Brainstorming Group
When are ransomware payments illegal under current U.S. law?**

1. Introduction

- a. The Brainstorming Group (“BG”) was tasked with exploring the development of a legal standard and/or factors by which to determine whether a threat actor to whom one is considering making a ransomware payment either is itself, or is acting for the benefit of, an organization/entity listed on OFAC’s Specially Designated Nationals and Blocked Persons List (SDN List), or from a country under comprehensive OFAC embargo, such that making a ransomware payment to that threat actor would be prohibited.¹
- b. As set forth in the BG’s Charter, the International Emergency Economic Powers Act (IEEPA) and the Trading with the Enemy Act (TWEA) make it illegal, “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 [i.e., is an organization/entity listed on the SDN List], 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 [i.e., an organization/entity listed on the SDN List].” A violation of these laws can result in civil and/or criminal penalties.
- c. Further, there is currently no legal authority that guides determination of whether a cybersecurity threat actor that is demanding a ransomware payment is itself listed, or even if not listed is nonetheless acting for the benefit of an entity that is listed, on the SDN List. As a result, ransomware victims and the organizations that assist them in communicating with such threat actors are left to interpret the regulations and some related guidance to arrive at the answers to these questions and are at risk of violating the law if they come up with the wrong interpretation. They therefore have little independent third-party guidance in determining whether their ransomware payment to a specific threat actor violates the law. Moreover, much of the guidance that OFAC has issued with respect to diligence of potential SDNs is focused on assessing commercial counter-party risks rather than attribution around criminal and nation-state actors, which take extensive measures to obfuscate their identities and activities. The lack of clarity has also led to differing conclusions as to whether a specific threat actor is listed, or acting on behalf of someone else who is listed, on the SDN List.

¹ Making a payment in this context covers a broader set of activities than simply transferring funds. It may include all manner of facilitation of such payments, including by third parties.

- d. The BG has therefore considered whether WG11 should develop an independent standard and/or factors that would provide guidance on this issue. The BG has evaluated how issues of this sort have been handled in other legal contexts and draw from those contexts in developing any standard or factors for consideration.
- e. The BG's outline of its work and recommendation is set forth below. This outline is not "final" in any sense, but instead is a work in progress that represents the thinking of the BG to date. We ask that other members of WG11 provide feedback, which we anticipate will be critical to the development of final conclusions on the issues presented.

2. Summary of Recommendation

The BG recommends that WG11 form a drafting group to develop a work product that would provide independent guidance for assessing risks and potential liability arising from a ransomware payment.

3. Intended Audience

- a. Who needs this work product?
 - i. Incident-response teams
 - ii. Persons and entities who experience a ransomware incident
 - 1. Directors, officers, and management personnel
 - 2. Information security personnel
 - 3. In-house counsel and compliance/privacy officers
 - iii. Outside counsel
 - iv. Cybersecurity and incident-response vendors and consultants
 - v. Companies involved in facilitating negotiations with ransomware threat actors and making cryptocurrency payments
 - vi. Insurance carriers
 - vii. Post-incident regulatory and legal professionals
 - 1. Counsel
 - 2. OFAC and other regulators
 - 3. Courts
 - viii. Legislators
- b. Why do they need this work product?
 - i. Risks associated with ransomware payments are often unclear.
 - 1. Risks need to be assessed quickly, usually within 1-3 days.
 - 2. Many victims are ill-equipped to understand the risks or implications of ransomware, and lack resources to hire sophisticated counsel and vendors.
 - 3. Pre-payment attribution and identification of threat actors ("TAs") is difficult and sometimes unfeasible.

4. OFAC guidance is mostly limited to post-ransomware-payment enforcement guidelines, and a general soft-recommendation against making payments (echoed by law enforcement).
 - ii. Substantive issues are rarely decided.
 1. OFAC's enforcement work is mostly non-public
 2. Few OFAC enforcement actions are litigated in court, leaving little guidance as to the scope of regulatory powers and whether OFAC has overstepped.
 - iii. Current guidance is limited to OFAC's perspective.
4. Outline of potential work product
 - a. Background
 1. Introduction of ransomware and impact
 2. Typical structure of incident response and relevant parties
 - b. Relevant legal and regulatory standards
 1. TWEA and IEEPA overview
 2. OFAC regulations
 - c. OFAC guidance
 1. Current OFAC guidance and enforcement guidelines appear to adopt a "strict liability" or similar standard for any ransomware payment made to a threat actor ("TA") on the SDN List.
 - a. 31 CFR App'x to Part 501, III(B) (assessing knowledge or "reason to know" not as elements of liability but rather as factors affecting enforcement: "Generally, the greater a Subject Person's actual knowledge of, or reason to know about, the conduct constituting an apparent violation, the stronger the OFAC enforcement response will be.")
 - b. "Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments" (U.S. Dep't of the Treasury, Oct. 1, 2020), available at https://home.treasury.gov/system/files/126/ofac_ransomware_advisory_10012020_1.pdf
 - c. "Updated Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments" (U.S. Dep't of the Treasury, Sept. 21, 2021), available at https://home.treasury.gov/system/files/126/ofac_ransomware_advisory.pdf ("OFAC may impose civil penalties for sanctions violations based on strict liability, meaning that a person subject to U.S. jurisdiction may be held civilly liable even if such person did not know or have reason to know that it was

engaging in a transaction that was prohibited under sanctions laws and regulations administered by OFAC.”)

2. In other words, a ransomware victim may be liable for sanctions-related penalties resulting from a ransomware payment, even if the victim did not know or have reason to know that the TA was on the SDN List or was connected with an embargoed country (such as Iran, North Korea) at the time of payment.

d. Issues arising from OFAC guidance

1. Complying with OFAC position is challenging

- a. Attribution can be difficult
- b. Timeframes are typically very short
- c. Strict liability cannot account for those concerns

2. OFAC does not consider mitigating factors in the liability determination, only for the enforcement process

- a. Willful or reckless violation
- b. Awareness of conduct
- c. Harm to Sanctions Program Objectives
- d. Individual Characteristics (sophistication, size, volume)
- e. Compliance Program
- f. Remedial Response
- g. Cooperation
- h. Timing of violation (with respect to the addition of SDN or change in regulation)
- i. Omnibus

3. OFAC position generates uncertainty and a potential chilling effect for key players.

- a. Insurers
 - i. Unclear situations with risk / uncertainty

ii. Might cause rejection of payment in legitimate situations

b. Incident Response Teams

i. Often needed to facilitate payment but are part of the risk chain

c. Could OFAC position lead to more non-US based IR / negotiators?

i. Target victim retains risk - but would non-US negotiator potentially provide more options and not be subject to OFAC penalties?

d. Legal Teams (Internal / Outside counsel)

i. OFAC has not ruled out attorneys facilitating payments facing potential liability.

ii. Potential ethical considerations

e. Is OFAC's strict liability position a correct interpretation of the law?

1. TWEA includes an express requirement that the alleged violator have "**knowledge or reasonable cause to believe** that [the party on the other side of a transaction] 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." 50 U.S.C. § 7303 (emphasis added).

2. IEEPA does not include a similar "knowledge or reasonable cause to believe" standard in the civil context, but it only imposes liability for a violation of a specific order or regulation issued pursuant to its grant of authority. See 50 U.S.C. § 1705.

a. Many of those orders or regulations appear to impose "strict liability" in the sense that they do not have a specific *mens rea* requirement. However, most of the orders and regulations do not necessarily bar every possible transaction with a sanctioned person or entity. Instead, the prohibitions are typically more specific.

i. For example, EO 14065 (recently issued in connection with the Ukraine-Russia conflict) prohibits, among other things:

(i) new investment in the so-called DNR or LNR regions of Ukraine or [other "Covered Regions"] by a United States person, wherever located;

(ii) the importation into the United States, directly or indirectly, of any goods, services, or technology from the Covered Regions;

(iii) the exportation, reexportation, 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

(iv) 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.

b. Many of the regulations also include affirmative defenses or safe harbors that are tied in some way to the knowledge of the alleged violator.

i. For example, 31 CFR 589.202(d) provides (emphasis added): Transfers of property that otherwise would be null and void or unenforceable by virtue of the provisions of this section shall not be deemed to be null and void or unenforceable as to any person with whom such property is or was held or maintained (and as to such person only) in cases in which such person is able to establish to the satisfaction of OFAC each of the following:

(i) 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);

(ii) 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

(iii) 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 [the transfer was unlawful].

c. Some regulations, however, do not impose strict liability. *See Epsilon Elecs., Inc. v. U.S. Dep't of the Treas., 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).

d. In addition, IEEPA requires a showing of willfulness for criminal liability. *See* 50 U.S.C. § 1705(c).

3. Similar legal standards in other contexts

a. SBA Loan Fraud – 13 CFR 142.6

i. A person knows or has **reason to know** (that a claim or statement 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.

b. Could this standard (or something similar) be appropriate in the ransomware context?

i. Perhaps a ransomware victim should not be able to avoid liability by remaining deliberately or willfully ignorant or by acting in reckless disregard of existing facts, but should it be required to conduct a time-consuming and expensive investigation in order to gain 100% confidence that a threat actor is not on the SDN list?

(i) 100% confidence might not be possible.

(ii) Lives might be at risk while the investigation is ongoing.

4. Other considerations

a. Does OFAC’s position in some/all cases provide fair notice under Due Process Clause of the Fifth Amendment to the U.S. Constitution? *See Exxon Mobil Corp. v. Mnuchin*, 430 F.Supp.3d 220 (N.D. Tex. 2019).

f. Licensing Option

- i. OFAC specifies the ability to apply for a specific license
- ii. Three references to licensing in Enforcement Guidelines
 1. Filing of a license application does not constitute voluntary self-disclosure
 2. Denial, suspension, modification, or revocation of a license as possible OFAC responses to an apparent violation
 3. Whether conduct constituting apparent violation would have been licensed by OFAC to be considered in evaluating harm to sanctions program as part of determination of appropriate administrative response
- ii. Anecdotal experience suggests licensing has not been useful
 1. Not aware of any licenses granted in ransomware context
 2. Even denials have taken months (up to six months) and some have also reported no response at all
- iii. OFAC position
 1. Publicly, OFAC has a presumption against licenses in the ransomware context (Sept. 21, 2021 Updated Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments)
 2. Private Interviews Conducted by BG
 - a. Confirmation that no license has been approved in ransomware context, though also noted that the number of applications has been relatively small
 - b. Indicated that OFAC motivated to use expedited/streamlined process for ransomware applications given national security/foreign policy inherently at issue
 - c. Conceded that in order for applicant to rebut presumption, must be a “very compelling foreign policy/national security interest”
- iv. Feasibility of using licensing process to obtain timely approval for making ransomware payment
 1. Timing may not be the primary hurdle given potential for expedited process and the ransomware negotiation period being extended from 5 days to 8 days based on one recently-published law firm’s 2021 statistics (per an April 7, 2022 SEC Media, “Ransomware negotiations are taking longer (and that’s a good thing)”)
 2. But appears very hard to rebut the presumption so this is likely where the fatal hurdle is with respect to getting pre-authorization to pay ransom payment
- v. Potential value of license application notwithstanding above
 1. Contrary to Enforcement Guidelines, the Enforcement Division Assistant Director indicated that an application for license could be

viewed as a voluntary self-disclosure depending on content/thoroughness

2. Therefore, contemplate whether going through licensing application while negotiating payment might still have some value for post-violation enforcement proceedings

g. Two potential frameworks for assessing risk of ransomware payments

- i. Outcome 1: Outline a reasonable, best practice process for attribution. This helps to define the risk of making a payment under the OFAC strict liability position.
 1. This framework assumes OFAC strict liability as the standard and would assist organizations in working to quantify their level of risk in making a ransom payment.
- ii. Outcome 2: Outline a reasonable, best practice process for attribution. Where attribution is unclear or suggests a banned actor is involved, include factors to consider in determining whether a ransom payment might still be considered reasonable
 1. This framework is a reasoned alternative to the OFAC strict liability model

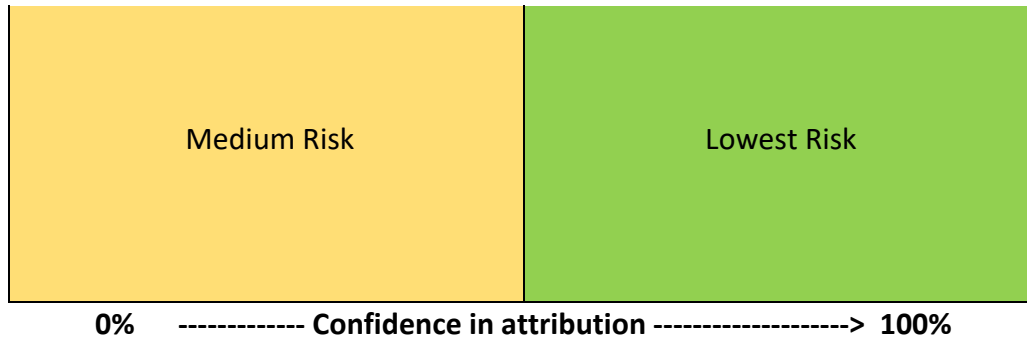
5. Framework for Outcome 1

- a. Attribution – reasonable inquiry process
 - i. One attribution approach is to leverage threat intelligence 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 on the OFAC SDN list²
 1. Filing of IC3 reports is encouraged
 - a. Provides FBI/law enforcement with more information and demonstrates good intent
 - b. Law enforcement can sometimes provide additional insights
 2. Blockchain analysis
 - a. Analyze transactions associated with the cryptocurrency wallet
 - b. Cross check wallet provided by threat actor, and any wallets associated with the provided wallet, against the OFAC SDN and other global watchlists
 - c. Check internal database for previous transactions and validate with blockchain analysis tool
 3. Endpoint detection and response hits
 - a. Analyze detections from the client’s existing EDR solution, or deploy one to the client’s environment

² This approach was developed by Arete Incident Response.

- b. Cross check list of detected malware/trojans against government repositories (OFAC/DOJ)
 - 4. Cyber threat intelligence analysis
 - a. Cross-check ransomware variant indicators of compromise (variant itself, Internet Protocol/email headers, methods of infiltration and behavior in the client's environment)
 - b. Intelligence sources
 - i. Security operations center (SOC) database maintained by many incident response / threat intelligence firms
 - ii. Dark web
 - iii. Open source intelligence from security researchers
 - 5. All information is synthesized into a report to allow counsel and client to make go/no go decision
 - 6. Examples
 - a. Go decision was made when it was shown that apparently banned threat actor had sold the variant, the variant sale was discussed on the dark web, and the indicators of compromise were completely different from those used previously by the banned TA
 - b. Intelligence gained from the recent release of information by the Ukrainian members of the Conti ransomware group provided new information that one of the leaders of the group resided in the Crimea, a banned area, and that other threat group activities were occurring within Crimea, which resulted in the halt of facilitation of further payments to Conti
- ii. Other examples
 - b. Define the risk level based upon the attribution process
(More attribution information moves X axis further to right;
More direct identification of bad actor on SDN list moves Y axis further up)





- i. Lowest Risk
 - 1. Some / many factors are available to assess attribution
 - 2. Attribution suggests bad actors who are not on SDN
 - 3. Example
 - a. Blockchain, endpoint analysis, threat intelligence factors all point to XYZ Group. XYZ Group not on the SDN List
- ii. Medium Risk
 - 1. There are few factors available to assess attribution
 - 2. Attribution suggests bad actors who are not on SDN
 - 3. Example
 - a. New malware variant, only attribution indicator is blockchain analysis pointing to relationship to XYZ Group. XYZ Group is not on the SDN List
- iii. Medium to High Risk
 - 1. Low to medium number of factors available to assess attribution
 - 2. Factors may suggest an SDN actor or one operating from an embargoed country (such as Iran, North Korea)
 - 3. Example
 - a. Bad actor not on SDN but evidence some linkage to SDN (eg prior transactions; possibly re-forming an old group, malware similarities, etc.)
- iv. Higher Risk
 - 1. Some / many factors available for attribution
 - 2. Factors suggest a likely SDN actor, or one operating from an embargoed country (such as Iran, North Korea)
 - 3. Example
 - a. Blockchain, endpoint analysis, threat intelligence factors all point to ABC Group. ABC Group is on the SDN List
- c. Evaluate the risk and assess any mitigating factors
 - i. Risk level informs risk of liability under OFAC (TWEA/IEEPA)

- ii. Mitigating factors inform the risk of penalties (not liability)
- iii. Document information known at the time

6. Framework for Outcome 2

- a. Follow attribution process and risk assessment as outlined for Framework 1
 - i. Responsibility is based upon “reasonable inquiry”
- b. If “reasonable inquiry” suggests SDN actor, assess mitigating factors
 - i. OFAC defined list (provided in prior section)
 - ii. Other mitigating factors
 - 1. Potential for loss of life or health
 - 2. Loss of jobs / regional or national economic damage
 - 3. Critical infrastructure impact
 - 4. Taxpayer interest (City of Baltimore example)
 - 5. Attenuation considerations
 - a. How far removed does the bad actor need to be from a known SDN?
 - b. Example: Group conducting the attack is not on SDN but possibly uses SDN’s services / malware
 - i. Fully paid / pre-existing relationship (i.e. paid for malware or ransomware related services in full prior to the attack)
 - ii. Contrast with an ongoing relationship (monthly fee or even a percentage split)