

The Sedona Conference Draft Commentary on Ransomware Payments (October 2022)



The Sedona Conference Commentary On Ransomware Payments

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

**Confidential draft to be presented at the Midyear Meeting
on November 2, 2022**

Author: The Sedona Conference

Drafting Team Leader: Jim Shook

Drafting Team

Guillermo Christensen	John Gray
Eric Gyasi	Bill Hardin
Emily Jennings	Robert Kirtley
Jon Polenberg	Daniel Raymond
Larry Wescott	Zachary Willenbrink
Phil Yannella	

Steering Committee Liaison: Al Saikali

I. Introduction

Organizations throughout the world are being victimized by ransomware attacks¹ where threat actors encrypt data and applications, causing an abrupt stop to or degradation in an organization's ability to conduct business. These threat actors then demand a ransom payment in return for a decryption tool used to regain access, and increasingly also attempt to extort victims by threatening to publicize stolen data. Ransomware attacks can result in substantial costs and even risks to life. Determining whether to pay a ransom or work to recover systems without access to the decryptor tool is a difficult and often expensive decision.

In the United States, no Federal laws² have been enacted specifically to limit the payment of cyber ransoms.³ However, the Office of Foreign Assets Control (OFAC) has ("OFAC") has sought to restrict the payment of ransoms to certain parties and to certain embargoed countries, relying on two core national security laws that are heavily relied on by the U.S. Government to regulate international trade and national security. Specifically, the Trading With The Enemy Act (TWEA) and International Emergency Economic Powers Act (IEEPA) prohibit U.S. persons from trading or attempting to trade with an enemy or ally of an enemy of the United States. OFAC has extended its long-standing position that U.S. persons are strictly liable for a civil violation when they make a payment to a blocked person or deal with an embargoed country. Strict liability in this context means that any U.S. person may face a civil enforcement action by OFAC even in a situation where the U.S. person does not know or have reason to know that a ransomware payment is being made in violation. A willful violation of these laws can lead to civil and/or criminal penalties enforcement, which would be carried out by the Department of Justice, and requires a showing of intent.

But the strict liability standard may not apply in all cases. Indeed, TWEA states that an alleged violator must 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. § 1705. In contrast, IEEPA does not include similar "knowledge or reasonable cause to believe" language and many of the executive orders and OFAC regulations issued pursuant to the IEEPA do not have a specific *mens rea* requirement. However, even under IEEPA, some orders and regulations do not appear to impose strict liability, and such a standard could be subject to challenge in some cases.

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 There are now a number of state laws which restrict the ability of certain organizations to pay cyber ransoms.

³ The Federal government has imposed rules for certain organizations, primarily 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 US Department of Treasury's FinCEN.

Moreover, the strict liability approach is not well suited to meet the goals and nuances of decisions regarding the payment of cyber ransoms. It is almost always difficult to understand which organization is receiving a ransomware payment, even months after a payment has been made, and time pressures and obfuscation by threat actors make the attribution process even more difficult. In addition, some scenarios, such as risk of physical harm or large-scale economic disruptions, suggest that making a ransom payment might be the lesser of evils in certain cases and that some allowance should perhaps be made in those scenarios.

This paper reviews these issues in three parts:

Part 1

An analysis of TWEA and IEEPA and whether OFAC's interpretation of strict liability under these Acts is legally well supported;

Part 2

A framework for assisting organizations in attributing the source of an attack and likely recipient of a ransom, and evaluating their level of risk from OFAC if they elect to pay; and

Part 3

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

II. Current Legal Framework

a. Background and Current OFAC Guidance

TWEA and IEEPA prohibit U.S. persons from trading or attempting to trade with an enemy or ally of an enemy of the United States. A violation of these laws can result in civil and/or criminal penalties.

These laws prohibit U.S. Persons from dealing in the property of any sanctioned persons which in some cases extends to an entire embargoed country, such as Iran or North Korea. The Office of Foreign Asset Controls (OFAC) enforces sanctions civilly and maintains the Specially Designated Nationals and Blocked Persons List (SDN List). There are also several countries and regions that are under comprehensive OFAC embargoes (together, Sanctioned Parties).

With respect to ransomware payments, there is no specific OFAC sanctions program targeting ransoms -- instead the prohibitions primarily affect specific cyber threat actors, connected to nation states (Evil Corp, Lazarus) and more recently sanctions on certain exchanges for cryptocurrency that have been used by ransomware threat actors to transfer funds. Despite the presence of well-known criminal gangs operating in the ransomware space, OFAC has not yet sanctioned a group without there being a nation-state nexus. For example, Conti, one of the most prolific ransomware groups operating primarily out of Russia and Eastern Europe, was not

sanctioned by OFAC before it reportedly disbanded itself in the aftermath of an internal dispute over Russia's invasion of Ukraine.

However, as ransomware schemes have proliferated in recent years, it has become increasingly difficult to determine whether a threat actor is itself or is affiliated with a Sanctioned Party—a process this paper refers to as “attribution” in the intelligence and cyber response communities. Attribution is particularly difficult in the context of cybersecurity threat actors, who: engage in criminal activity; sometimes may act on behalf of (or with the tacit approval of) nation states; and generally take extensive measures to obfuscate their identities and activities.

In fact, OFAC's approach to designating certain groups relies on traditional definitions for the sanctioned person—for example, including the names of individuals known to be affiliated with a particular threat actor, such as Evil Corp, or the name given to their malware (e.g., Dridex). OFAC has also identified digital wallet addresses for certain threat actors. OFAC has not, however, attempted to define any threat actor with reference to a particular type of code being used in the malware (other than by the moniker used by incident responders) that would allow a forensic team to identify the software or platform being employed to launch the ransomware attack.⁴ These characteristics used by OFAC are therefore of limited use to incident responders attempting to attribute a ransomware attack.

There are also no judicial decisions or case law that directly address OFAC sanctions or enforcement in the ransomware context.⁵ And, although OFAC has issued two advisories focused on ransomware, those advisories provide little guidance on identifying Sanctioned Parties. Most attribution must therefore be done with reference to practices that are primarily of use in assessing risks in legitimate commercial transactions where it is unclear whether a counterparty to the transaction is a Sanctioned Party. As a result, ransomware victims (and third-party service providers who help them) are often unsure of the attribution of the threat actor targeting them—leading to a lack of clarity regarding the legality of a given payment under TWEA and IEEPA and thus further complicating the analysis of whether to pay a ransom.

In addition, the two OFAC advisories (issued in 2020 and 2021) pointedly note the risk that incident responders face from OFAC's “strict liability” standard. Specifically, those advisories explain:

OFAC may impose civil penalties for sanctions violations based on strict liability, meaning that a person subject to U.S. jurisdiction may be held civilly liable even if it did not know or have reason to know it was engaging in a transaction with a person that is prohibited under sanctions laws and regulations administered by OFAC.

⁴ Such code analysis is key to a more reliable attribution effort, and is typically what is relied on by threat analysts to attribute an attack to a particular actor. Other techniques may include “fingerprinting” the tactics used by the threat actor.

⁵ In related matters, there are several insurance disputes involving so-called war exclusion clauses. In these cases, insurers have argued that an attack by a nation state threat actor triggers the clause. Some carriers are expanding the definition of the war exclusion to explicitly include nation state attacks -- these cases may in a future scenario touch on OFAC issues to the extent that the threat actors may be connected to a nation state under a comprehensive OFAC embargo.

Further confirming OFAC’s “strict liability” approach, its Economic Sanctions Enforcement Guidelines (found at 31 C.F.R. Part 501, App’x A) specify that knowledge and intent factors will be considered only in determining the proper enforcement mechanism in a given case—not in the underlying analysis of whether a violation occurred. Thus, for instance, even a party who conducts a good-faith investigation to reach a well-reasoned determination that the threat actor is not a Sanctioned Party—though it may suffer a lighter punishment—is nonetheless liable for a violation if it is later determined that the threat actor is, in fact, a Sanctioned Party. OFAC underscores this point by speaking at length in both advisories to the steps a victim of ransomware can take to reduce the impact of an unintended violation of an OFAC sanction.

b. Does OFAC’s Guidance Comport with the Law?

Despite OFAC’s recent advisories and its enforcement guidelines, at least some of the laws and regulations that OFAC enforces do not appear to impose strict liability. As noted above, 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. *See, e.g.*, 50 U.S.C. § 4303(a) and (b). Likewise, although certain regulations under IEEPA may impose strict liability, at least some provisions of IEEPA itself and some of its associated regulations require knowledge or willfulness to establish liability. *See, e.g.*, 50 U.S.C. §§ 1705, 1708(b) and (d)(4). This suggests that OFAC’s interpretation of the scope of strict liability may be subject to some challenge by parties seeking to determine their potential liability for making a ransomware payment where they had no knowledge that the recipient was a Sanctioned Party.⁶

i. Legal Standards under TWEA

More specifically, 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

⁶ Among the authors of this paper, there is a difference of opinion regarding the import of OFAC’s strict-liability standard. On one side is a view that OFAC’s strict-liability approach has been tested through enforcement proceedings and is now well established, such that this paper should focus on the extent to which OFAC’s approach creates a particularly difficult situation for victims and incident responders in ransomware matters, where it is often infeasible to undertake diligence inquiries of the kind that are done in other commercial contexts to identify sanctions risks. The alternative view is that there are reasons to question the extent to which OFAC’s strict-liability approach holds water when the underlying statutes are carefully scrutinized.

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.

50 U.S.C. § 4303(a) through (c).⁷

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. *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 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.”)

ii. Legal Standards under IEEPA

⁷ 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 [see discussion in part iii below].

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].” 50 U.S.C. § 1705(a). Standing alone, that provision does not require any level of knowledge or intent before civil liability may be imposed. *See In re Criminal Compl.*, 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”). And many of the regulations or 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. *See, e.g.*, EO 14065, 87 Fed. Reg. 10293-96 (Feb. 21, 2022).

However, criminal liability may only be imposed for willful violations of IEEPA, *see* 50 U.S.C. § 1705(c), and the more 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 industrial espionage in cyberspace, of technologies or proprietary information developed by United States persons,” *id.* § 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.”).

Moreover, the regulations and orders issued pursuant to IEEPA do not necessarily prohibit every possible transaction with every person or entity on the SDN List. Instead, the regulations and orders are typically issued in connection with a specific conflict, series of events, or set of circumstances relating to a particular country, region, or group. *See, e.g., id.*; *see also* 31 C.F.R. §§ 501-598 and App’x.

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

- new investment in the so-called DNR or 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 EO 14065, 87 Fed. Reg. 10293-96.

Moreover, several regulations include affirmative defenses or safe harbors relating to the knowledge or intent of the alleged violator. *See, e.g.*, 31 C.F.R. §§ 578.202(d), 589.210(d). 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
 - (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.

31 C.F.R. § 578.202(d) (emphasis added).⁸

In addition, some of the regulations do not impose strict liability at all. *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).

iii. OFAC’s Guidance May Not Comport with the Law

Considering the foregoing, OFAC’s guidance appears to be insufficiently nuanced to the extent it suggests that any transaction of any kind with any actor on the SDN list automatically gives rise to liability under TWEA and/or IEEPA on a strict-liability basis. Some transactions may be subject to strict liability under those laws and the related regulations, but other transactions may not be.

⁸ 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).

c. 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 which 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 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 of 2021 Advisory that OFAC will apply a presumption against granting specific licenses in the ransomware context. 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 deference afforded OFAC by courts.

There are major hurdles to using the licensing process in the ransomware payment context. First, the victim must know the ransom payment is going to an individual SDN or otherwise implicates a sanctioned country, region, or government. Strong attribution to an SDN or sanctioned region in the beginning of a ransomware incident is nearly impossible due to the fog of war and the issues around attribution. Certainly, the victim could submit an online application without providing much information. But there is no reason to ask for a license from OFAC if the 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 (NLR) determination, which in itself can act as an assurance that the conduct for which a license was being 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 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 victims, however, are not in the position to wait months or years for OFAC's decision before making a payment. 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 need to make a ransom payment.

Absent FOIA, there are no publicly available statistics tracking license applications, but it is generally known that there have been very few specific licenses related to ransomware. Certain insurers have sought specific licenses to reimburse victims. These license requests are believed to be still pending, and it is believed that OFAC has not issued a specific license in the ransomware context.

The current license process is not a workable solution for insurers or others reimbursing ransom payments due to the speed of the process and OFAC's reluctance to weigh in on attribution, underscoring the fact that the current license process is not a feasible solution for ransomware victims concerned about OFAC enforcement.

d. OFAC's Position Generates Uncertainty

OFAC's initial foray into the cybersecurity/ransomware issues followed the attribution of a ransomware threat actor to groups connected to nation-states -- Evil Corp to Russia and eventually others to Iran and to North Korea. OFAC's designations of these state-sponsored or affiliated groups tracks closely to the overall mission for OFAC and, in the case of Iranian and North Korean hackers, is also in line with the comprehensive embargoes against those states. Iranian and North Korean threat actors moreover have largely specialized in non-ransomware criminal activity and, in any case, are not on the scale of Russian or Eastern European-affiliated threat actors, which are widely reported to be primarily responsible for much of the activity in ransomware.

After OFAC's designation of a handful of threat actors as SDNs between 2016-2019, OFAC took an exponentially more significant step in 2020 in issuing an advisory that cautioned victims and incident responders of the potential risks from paying a ransom to a group designated as an SDN or affiliated with an embargoed country. At the time of the 2020 advisory and the 2021 revisions, the number of SDNs listed by OFAC in connection with cyber attacks remained small relative to the overall SDN list.

To date, there are no reported instances of OFAC bringing an enforcement action against a victim or a third party for facilitating a ransom payment.

- Anecdotally, we are aware of instances in which law enforcement has contacted victims after a ransom payment to gather information where there are some indications that the threat actor was located or connected to an embargoed country.
- We also understand that some victims have reported incidents to law enforcement and to FinCen after the fact involving a potential SDN.
- We are aware of no instances in which a victim or their incident responders have sought a license to make an otherwise prohibited payment. Reportedly, some insurance carriers have sought licenses from OFAC to reimburse their insured when some attribution indicated an SDN may have been involved.

OFAC has also not provided much additional clarity around the two ransomware advisories - there are, for instance, no FAQs that address issues and questions, in contrast to those prepared

in response to compliance and practitioner questions for sanctions against Russia, Iran, or North Korea.

OFAC's approach instead appears calculated to inject uncertainty in the minds of victims and the incident response community when considering making a ransom payment. Rather than a wholesale prohibition on making a ransom payment, OFAC's approach to date has been to caution victims and incident responders that a payment to a sanctioned threat actor could result in an enforcement action and thereby dissuade payments without OFAC having to bear the burden of such a prohibition, and the potential negative publicity from victims being unable to recover their business operations.

Despite the lack of OFAC enforcement activity, incident responders, to date, have been affected across several dimensions:

- Almost all incident response companies have instituted some kind of OFAC compliance check process, starting with rudimentary checks of digital wallets against the SDN list (a largely feckless process given that the vast majority of threat actors create and dispose of wallets for each attack). Many of the OFAC compliance checks being done by incident responders or their counsel rely on mostly unreliable and unverifiable technical indicators -- the threat actors obfuscate first and foremost to avoid law enforcement and now to avoid 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 that are related to OFAC's advisory, 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 RaaS platforms, such as Conti, has further complicated the attribution for OFAC purposes; an affiliate could easily be located in Iran, yet use a Russian-based RaaS.
- Some incident response companies go so far as to ask the threat actors, during the negotiations for payments, to identify themselves as part of performing the OFAC check.
- Anecdotally, we also understand that some victims and incident responders prefer not to inquire into which threat actor group is involved under the mistaken theory that ignorance will present some defense or will make 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 they will authorize payment of a ransom under a policy.⁹

Under OFAC’s guidance, the implications for incident responders appear clear on the surface but in fact are problematic. On the one hand, the OFAC advisory appears to suggest that all the entities involved in incident response -- from breach coaches, 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. This can be done by instituting compliance checks and working with law enforcement. But the reality is that 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, which are typically not involved in ransomware incident response. This leaves the typical incident responder relying primarily on open source/public reporting or, in limited instances, whatever information is available from law enforcement.

This is in stark contrast to the kind of process that businesses in the US have implemented to comply with OFAC requirements, 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. These KYC processes fail frequently, such as incorrect spelling of names because of a system error, and such instances can still lead to liability.

A similar compliance approach to OFAC checks for ransomware is nearly impossible 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. OFAC’s ransomware-related designations primarily involve identifying certain digital wallets associated with a handful of threat actors, which, as noted above, is an almost completely useless approach given the disposable nature of these wallets. The other approach OFAC has taken is designating a “group” by a moniker such as “Evil Corp,” or by reference to a type of ransomware, such as Dridex, which is even less helpful since these groups are informal, constituted ad hoc, and often use specialists who may work across several groups or platforms.

For now, as long as the number of SDNs remains low, ransomware incident response will continue to grapple with questions about whether a threat actor could be sanctioned. To the extent that some associated data around an incident point in the direction of an embargoed country, we expect that there will be strong resistance to making payments unless there are highly extenuating circumstances, such as loss of life.

III. Assessing the Risk of Making a Ransomware Payment

a. Introduction

⁹ These attestations would likely do little to protect the carriers, if OFAC were to apply a strict liability approach.

If liability can attach under OFAC enforcement when making a ransomware payment, organizations should evaluate their risk in making such payment. For example, if the standard remains strict liability, to evaluate their OFAC risk an organization may conduct some investigation to attempt to determine the payment recipient. Even if a lower standard applies, such as “knowledge or reasonable cause to believe,” some level of diligence focusing on attribution is typically necessary, both to evaluate risk and potentially to assist in mitigating later enforcement from OFAC.¹⁰

This section provides guidance on appropriate steps to assist in the attribution process; along with a discussion on how the findings from that work, even if inconclusive, can inform the level of OFAC enforcement risk if a payment is made.

b. Attribution Process

The process of attributing the activities surrounding a ransomware attack to a given threat actor or crime syndicate (collectively “Threat Actor”) 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 victims to use.

The ransom note is the first line of identification. Threat Actor notes are customized to their brand. For example, the HIVE note states it is the HIVE threat actor and gives a Tor Node with the Hive Leak site and channel for communications. The notes are cataloged on many third-party sites and by law enforcement. Lastly, most Threat Actors have a leak site that they direct victims to use.

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 being used, 2) the internet protocol (IP) addresses used by the Threat Actor, 3) the attack kit used by the Threat Actor such as scanning tools, 4) the manner in which data exfiltration was performed by the Threat Actor (if applicable), and 5) talking to third-party sources such as law enforcement about the information identified during the investigation.

The encryption tool, if recoverable, provides many clues on the coding of the program. 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.

Once an agreement on payment is made with the Threat Actor, a cryptocurrency wallet identifier will be provided. The wallet is used as another indicator to determine whether a Sanctioned Party appears to be the intended recipient of the funds. Through forensic analysis, some wallets have

¹⁰ OFAC has identified mitigating factors to be used in the enforcement phase. See 31 CFR Ch. V pt. 501 App A

been tied to certain Threat Actors. Wallets are run through several programs that provide intelligence about the wallet being used, the cryptocurrency exchange, and other useful variables.

Another approach is to combine sources of information such as blockchain analysis, detections from the victim's 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.

The victim's anti-malware or endpoint detection and response system will contain indicators of compromise and/or malware signatures which 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 victim's environment, which can be matched against behavior patterns of other variants. Sometimes, information can be gleaned from reverse-engineering the malware.

Other sources of intelligence include the Incident Response firm's security operations center (SOC), the SOC of the EDR firm itself if it maintains one, 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, upon occasion, provided some valuable information.

Once payment is made, additional tracing of the wallet is generally not performed, as in the vast majority of instances, the Threat Actor simply creates a new wallet for each transaction. An exception would be if a Threat Actor re-ransoms a client for additional funds and provides a new wallet ID to the victim – in that instance, the original wallet ID would usually be re-analyzed.

c. Framework for Assessing Risk of Payment

The process of attributing a ransomware attack to a threat actor is as much art as science. Even 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, 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 pay a ransom. To help victims assess the degree of OFAC risk they may face for making a ransomware payment, this paper proposes a Framework to assist companies. Given the relative opacity of existing OFAC guidance, the lack of any OFAC sanctions to date against entities making payments to Sanctioned Parties as well as 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 the risk of liability, as well as enforcement, based on the standards and guidance provided by federal regulatory authorities to date.

i. 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 a company 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” – which is 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, notwithstanding questions regarding the legality of OFAC's stated position that payment to Sanctioned Parties gives rise to strict liability, OFAC's position will remain for the foreseeable future.

Second, the reasonableness of the steps an entity takes to attribute a ransomware attack to a threat actor do not factor into an analysis of the likelihood of an OFAC sanction. Reasonableness of a company pre-breach and post-breach actions, however, are potential mitigating factors that reduce the severity of any OFAC enforcement.¹¹

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

ii. Applying the Framework

Hypothetical One

A Fortune 100 retail company suffers a ransomware attack that significantly degrades its ability to timely process new online customer orders. The company has done 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

¹¹ OFAC has listed the factors that it will consider during enforcement. See 31 CFR Ch. V pt. 501 App A

affected servers. Company files an IC3 report and remains in regular dialogue with the FBI concerning the event.

The threat actor is not a known group, based on the contents of the ransom note. The company retains specialized ransomware negotiators to assist in assessing whether the threat actors are on the OFAC SDN list. By assessing indications of compromise, the 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 the threat actors provide for facilitation ransom payment. This analysis leads the experts to conclude there is a 50% that the threat actors are Iranian nationals.

Risk Assessment

Attribution Steps	Confidence Level	Inherent Risk	Mitigation Factors	Residual Risk
<ul style="list-style-type: none"> • Indications of compromise • Ransom note • Blockchain analysis • Threat intelligence 	50% that actors are Iranian nationals on the SDN list.	High	<ul style="list-style-type: none"> • Incident Response Plan • Regular training • Business continuity program • Notification to and regular communications with federal authorities 	Medium-High

Analysis:

This scenario involves a sophisticated company that undertakes substantial efforts to attribute a ransomware attack. Those steps reveal a high likelihood that the threat actors are on the OFAC SDN list. Therefore, ransomware payment to the threat actors is a clear violation of OFAC policy, giving rise to significant possibility of penalties based on OFAC's stated position.

However, the company has also undertaken substantial pre-attack steps to prepare for, avoid, and remediate a ransomware attack. The company also promptly notified federal authorities about the event and kept them regulatory informed. All of these are mitigating factors that lessen the likelihood of OFAC enforcement.

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 multi-factor authentication on relevant systems, pays for sophisticated anti-malware 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 timely responds to additional questions from the FBI.

The threat actor identifies themselves 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 provided for ransom payment, and concludes with 85% certainty that the threat actors are not on the OFAC SDN list.

Risk Assessment

Attribution Steps	Confidence Level	Inherent Risk	Mitigation Factors	Residual Risk
<ul style="list-style-type: none"> • Indications of compromise • Ransom note • Blockchain analysis • Threat intelligence 	85% that actors are not on the SDN list.	Low	<ul style="list-style-type: none"> • Basic cyber hygiene practices • Incident Response Plan • Notification to and regular communications with federal authorities 	Low

Analysis:

The ransomware victim is a small University lab that could have taken more pre-attack 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, ransomware payment to the threat actors is unlikely to violate OFAC policy.

Hypothetical Three

A medium sized software development company is the victim of a ransomware attack that results in the exfiltration 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 company 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 Info Sec department. The company had not done cybersecurity training for employees in several years. In fact, the company was surprised to learn that the data was even stored on local file shares as the company's policies required storage of customer data in a secure cloud environment.

In response to the ransomware attack, the company filed an IC3 report and reached out to local FBI agents, who provided very limited support and did not express significant interest in the attack. The company also retained a forensic consultant. The consultant examined indications of compromise and other forensic artifacts, including the ransom note, and determined that the malware was not associated with any known threat actor groups, including any groups on the OFAC SDN list. Because of cost constraints, the company declined to ask the consultant to do a blockchain analysis and proceeded to file necessary paperwork with OFAC and arrange payment to the threat actors.

Risk Assessment

Attribution Steps	Confidence Level	Inherent Risk	Mitigation Factors	Residual Risk
<ul style="list-style-type: none"> • Indications of compromise • Ransom note 	85% confident that threat actors are not on SDN list, but this is based on truncated forensic analysis.	Medium	<ul style="list-style-type: none"> • Some cyber policies; immature cyber program. • Violation of internal storage policies • IC3 report • FBI contact 	Medium

Analysis:

This hypothetical involves incomplete attribution efforts that are arguably justified by the significant danger to the company's business if payment was not made to the threat actors, given the lack of backups. While there is no clear indication that the threat actors are on the OFAC SDN list, the company could arguably have done more to confirm this assessment. The company's pre-breach mitigation efforts are, likewise, less than complete. The company'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 1C3 report and outreach to the FBI, whose lack of interest may itself have been an indication that the threat actors were low level and thus unlikely to have been on the SDN list. 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 company's mitigation efforts were poor and its attribution efforts could have gone further.

IV. Proposals To Advance the Law

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. Cyber intrusions have the hallmarks of the rare crime where the victim bears the brunt of the criminal activity and the regulatory sanction (or penalty associated) thereto – creating an untenable double bind.

This double bind may have entered into OFAC's calculus too, evidenced by the lack of any known enforcement against organizations making ransomware payments to restricted parties. But as previously discussed, even without enforcement, the OFAC position has a chilling effect upon legal counsels, boards of directors, insurers, forensic experts, and incident responders.

One significant ramification of the chilling effect is that at a vulnerable moment, an organization can be denied professional service advisors to fully advise and assist the organization. For example, in situations where the payment seems likely to reach a Sanctioned Party, professional advisors must decide whether to withdraw from the incident response, rehabilitation, and remediation process or risk sanctions as facilitators. The targeted organization is now further punished as a victim by restricting critical expertise when the organization is most in need. Further, the ambiguity of both the attribution of the threat actor and OFAC's enforcement can impact the likelihood of a prohibition under a cyber insurance policy.

To advance the law, consideration should be given to clearly delineated exceptions where ransom payments – based upon reasonable criteria that also advance public policy – should not be subject to OFAC enforcement or to a reduced version of enforcement.

This paper proposes two such exceptions.

b. Pre-Payment Notification Process

Considering that it is difficult to determine the recipient of nearly all ransomware payments, this commentary discusses changing where strict liability attaches. Rather than attaching strict liability to all payments, strict liability would be more consistent with a mandatory prepayment reporting regimen. Moving the strict liability triggering event to a prepayment report should eliminate OFAC's discretion as to whether to impose sanctions (using an ad hoc review into prepayment diligence). Imposing a prepayment report obligation would reduce the inconsistencies

inherent in comparing the reasonable “cause to know” standard under TWEA with the strict liability OFAC has interpreted for IEEPA (and TWEA, although it is not clear how).

A prepayment report would have to be filed no later than 24 hours¹² before making the ransomware payment-- in essence accelerating the normal filing of a Suspicious Activity Report with FinCEN such that the information would be more actionable. The reporting regimen would be similar to the currency transaction reporting obligation imposed on all people who handle cash transactions that exceed the reporting threshold. Likewise, all prepayment reports would be filed with OFAC and FinCEN. The prepayment report must 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, demanded the payment, and all other identifying information. Information about the ransomware payment should include the identify and verification of the hosted wallet¹³ person who will engage in transactions with unhosted¹⁴ or otherwise covered wallet counterparties. But a prepayment report should not be necessary for a ransomware payment made in convertible virtual currency or a digital asset with legal tender status exchanged between financial institutions regulated under the Bank Secrecy Act, except for any such financial institution in a jurisdiction listed on OFAC’s SDN List.

The prepayment reporting obligation would include an anti-structuring proscription. A person structures a ransomware payment when, either acting alone or in conjunction with or on behalf of other persons, they conduct or attempt to make a ransomware payment on one or more days in any manner to evade the reporting requirements. The term “in any manner” would include breaking down a single payment that exceeds the mandatory reporting threshold into smaller payments.

A person who files a prepayment report, including those who provide support services or insurance coverage and engaged in good-faith efforts to determine the nature of the ransomware attack, are not subject to liability.

It is worth noting that the prepayment reporting obligations would not modify the cash transaction reporting obligation. The value of a person’s convertible virtual currency, or a digital asset with legal tender transactions, is not relevant to determining whether the currency transactions in aggregate require filing a cash transaction report.

¹² A prepayment report should be updated upon any material change in circumstance or knowledge prior to payment being made. However the update does not restart the 24 hour waiting period.

¹³ Hosted wallet means that certain financial institutions provide custody services for their customers’ convertible virtual currency

¹⁴ Unhosted wallet means storing the private key for convertible virtual currency in a software program or written record to conduct transactions privately rather than using the services provided by a financial institution.

The prepayment report would not prevent OFAC or FinCEN from verifying the validity of a prepayment report. Filing a prepayment report does not relieve the payor from complying with any other provision of law.

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. While there should be little dispute that combating terrorism by cutting off funding to the perpetrators is important, threatening a ransomware attack victim under the strict liability standard has not demonstrably ebbed ransomware attacks. A prepayment reporting process would be preferable to suffering catastrophic data loss to avoid OFAC prosecution.

Imposing a prepayment report requirement would also increase ransomware attack disclosure, providing the government with quick attribution information. Under the current framework, victims may not report ransomware attacks at all or delay their reports, such that the information is more remote and less useful.

c. Responsible Preparedness Safe Harbor

i. Introduction

Some organizations attempt to resolve the double bind of being a victim and potential enforcement target by initiating cyber security resiliency measures to increase their security posture to ward off, limit the scope, and recover from cyber intrusions. To assist organizations with those efforts and to promote the public policy goal of increased cyber resiliency, responsible actions taken by an organization to prepare for an attack, and responsible actions taken after the attack, should be considered in determining potential culpability from OFAC. Note that these responsible actions would be considered in determining whether liability from OFAC should attach at all – and not merely in determining penalties in the enforcement phase.

A “safe harbor” test seems to be the best path forward. Historically, safe harbors have been viewed as a legal action an organization can take to minimize or remove a specific legal liability that would otherwise attach for such action. In the ransomware payment scenario, compliance with the terms of a safe harbor would protect an organization solely from OFAC enforcement, and not provide safe harbor from litigation or any other federal, state, or administrative agency regulatory liability or any other issue.

A safe harbor test creates a number of benefits:

- Provides certainty on whether an organization is safe from OFAC enforcement.
- Subject to the requirements listed in the test, advances public policy by providing an incentive to be more prepared to defend and/or better recover from a ransomware attack.
- Provides incentives for more open reporting and notification to law enforcement and interested parties.

The proposed safe harbor test encompasses the below listed factors. The implementation of these factors will account for organizational differences in sophistication, funding, personnel, and other real-world issues by organizations that often limit adoption of controls. To meet that concern, the safe harbor test utilizes a three-year annual gross revenue as a proxy for those factors, with enhanced implementation requirements as revenue levels increase.¹⁵

For this test, organizations are split into three groupings

- Large to Ultra-Large Business. Both for-profit and non-profit organizations¹⁶ with an average annual gross revenue for the preceding three fiscal years greater than \$250 million.
- Small to Medium-Size Businesses. For-profit and non-profit organizations with an average gross annual revenue for the preceding three fiscal years greater than \$100 million and equal to or less than \$250 million.
- Emerging Businesses. For-profit and non-profit organizations with an average gross annual revenue for the preceding three fiscal years less than \$100 million.

ii. Application

We propose that an organization may obtain a ransom payment safe harbor from the OFAC regulations if that organization has taken meaningful material steps to align that organization's cyber security resilience and protection with reasonable best practices.

Organizations must take specific measures, based upon their classification listed above, as follows:

Factor	Requirements
A. Governance	All organizations, regardless of size, shall (i) name a qualified individual to implement and supervise the organization's information security program, (ii) develop written cyber security policies and procedures, (iii) draft an incident response plan, and (iv) provide an annual certification of compliance to the Board of Directors (or the appropriate ownership control group).

¹⁵ While basing the test on a revenue amount can seem arbitrary, it provides a rough level of accountability and follows a structure used in some other safe harbor provisions. Perhaps most important, a quantifiable revenue number provides more certainty regarding the level of requirements that an organization must meet to qualify.

¹⁶ This paper does not take a position on whether Federal, state or local entities should be protected in the safe harbor.

Factor	Requirements
B. Technical Safeguards	<p>Emerging Businesses shall implement (i) multi-factor authentication for network access and email client access and (ii) password control protocols.</p> <p>Small to Medium-sized business shall implement the foregoing technical safeguards and implement (i) multi-factor authentication for production and developer servers, (ii) access privileges and identity management, (iii) endpoint detection and monitoring, and (iv) routine and regular patching protocol.</p> <p>Large to Ultra-Large Business shall conduct the foregoing technical safeguards and 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.</p>
C. Risk Assessments	<p>Emerging Businesses shall conduct annual penetration testing;</p> <p>Small to Medium-sized businesses shall conduct the foregoing risk assessments and conduct: (i) asset inventory, (ii) data classification and criticality rating assessment, and (iii) vulnerability scanning.</p> <p>Large to Ultra-Large businesses shall conduct the foregoing risk assessments and conduct: (i) cloud configuration assessments, (ii) network assessments and mapping, and (iii) annual vulnerability scanning.</p>
D. Controls	<p>Emerging Businesses shall conduct annual tabletop exercises;</p> <p>Small to Medium-sized businesses and Large to Ultra-Large businesses shall conduct the foregoing controls and implement: (i) 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.</p>
E. Post-Incident	<p>All organizations, regardless of size, shall file timely notification (e.g. IC3 notifications) to appropriate law enforcement entities and extending cooperation to such law enforcement entities during any investigative process (e.g., sharing of indicators of compromise).</p>

During a cyber intrusion event and before a ransom is paid, an organization that seeks the protection of this safe harbor must prepare a certificate signed by a senior executive¹⁷ tasked with legal and compliance matters attesting to the organization's: (i) preceding three-year gross annual revenue average and (ii) adherence to the above listed safeguards (inclusive of any

¹⁷ Smaller organizations without formal structures should identify an owner, large shareholder, executive officer or other senior individual for this requirement.

required certificate thereto). Such certificate shall be maintained by the organization for production upon request by the OFAC

V. Conclusion

OFAC's position on strict liability for civil enforcement around payments to a SDN, whether for ransomware or other dealings in property under TWEA and IEEPA may be subject to challenge in the view of some members of the drafting group. Other members of the drafting group view the issues around strict liability in the civil enforcement context as settled through enforcement precedent. Under either perspective, the lack of clear guidance from judicial decisions and the one-sided perspective on enforcement, from OFAC, complicates the environment facing incident responders, legal teams, negotiators and insurers.

A better path forward, at minimum, is to provide organizations with the ability to fully assess their risk of making a ransom payment within the strict time limits involved in ransomware attack scenarios. This may take the form of persuading OFAC to shift away from the strict liability interpretation to a more reasonable knowledge expectation based upon attribution activity; and/or a safe harbor which can encourage and enhance cybersecurity controls for all organizations.