Fighting Ransomware in the Dark: The Problem with OFAC's Strict Liability Threat for Ransomware Payments

Patrick Amano Dolan[*]

Introduction

A lawyer is the founder and owner of a small law firm. After years of investment and relationship building, she builds her business into a respectable practice with fifteen attorneys helping people throughout the community. Over several years, thousands of clients entrust the firm with their sensitive information, which the firm stores on its office computers.

One day, after coming into her office, the lawyer opens her computer to a message: "Your network has been penetrated and all files have been encrypted. Transfer a payment of $50,000 in Bitcoin to the wallet attached to the QR code below within 3 days. Sensitive documents will be released to the public if you do not pay."

The lawyer is concerned. Without network access, the firm will likely miss several of its upcoming court filing deadlines. Further, she realizes that if the clients' information were leaked, the firm would be exposed to a significant liability risk. These factors, in combination with the likely reputational harm, lead the lawyer to one conclusion: if she does not pay the ransom, it may be the end of her business.

Before paying the ransom, however, the lawyer quickly conducts research and discovers that a little-known sub-agency of the Department of Treasury, the Office of Foreign Asset Control ("OFAC"), threatens to punish victims of ransomware attacks with civil penalties for payments to entities on the agency's Specially Designated Nationals and Blocked Persons List ("SDN List").[1] The policy's strict-liability basis raises more concerns:[2] even if the victim did not know, nor reasonably should have known, that their attacker was on OFAC's SDN List, the agency may nevertheless impose hefty civil penalties. Since the policy's introduction

* J.D. 2024, George Mason University Antonin Scalia Law School; B.A. 2018, University of Virginia. Thank you to my family, friends, professors, mentors, and the *George Mason Law Review* editors for your support throughout this process.

1 OFF. OF FOREIGN ASSETS CONTROL, U.S. DEP'T OF THE TREASURY, UPDATED ADVISORY ON POTENTIAL SANCTIONS RISKS FOR FACILITATING RANSOMWARE PAYMENTS 1 (2021) [hereinafter OFAC ADVISORY], https://perma.cc/EW8R-87QJ.

2 *Id.*

in October 2020, however, the lawyer notices that the agency has yet to follow through on its threat.[3]

The lawyer weighs her options. To face an OFAC penalty, (1) the attacker must be on the SDN List and (2) OFAC must discover the payment. Given that OFAC has yet to bring an enforcement action under this policy, she assumes that the probability of an OFAC penalty is low. On the other hand, the firm will almost certainly suffer immediate and irreparable harm if she does not pay the ransom. Given these two options, the lawyer decides to pay the ransom and cover up the attack.

The lawyer quickly raises the funds, converts the money into Bitcoin, and sends the ransom to her attacker. Within a few hours, the computers are decrypted, and the firm continues its usual operations. Meanwhile, the attacker, emboldened by the successful attack on the lawyer, repeats the scheme several times to other small firms throughout the country. Faced with the same risks as the lawyer, each firm decides to pay the ransom and cover up the attack. The attacker continues to profit, and the government continues to be oblivious. Rinse and repeat.

The lawyer's dilemma is not unique. Thousands of U.S. organizations fall victim to anonymous ransomware attackers each year, yet only about 25% of attacks are reported to the government.[4] To address this dearth of crucial information, Congress created the Cyber Incident Reporting for Critical Infrastructure Act of 2022 ("CIRCIA"), which implements a cooperative mandatory reporting program with liability protections for organizations victimized by ransomware attacks.[5] OFAC, however, has taken the opposite approach by threatening to punish victims for payments to attackers on its SDN List.[6] In doing so, OFAC contradicts the cooperative approach under CIRCIA and disincentivizes victims, like the lawyer, from sharing information on their ransomware attacks with the government. The amount of influence wielded through this little-known sub-agency's policy begs the question: Is it lawful?

This Comment argues that the answer is no. First, the policy is not authorized by the statute in which it claims authority, the International Emergency Economic Powers Act ("IEEPA"), as it conflicts with the statute's plain text, legislative intent, and central purpose. Second, from a separation-of-powers perspective, the policy is unconstitutional as it conflicts with Congress's prescribed mechanism for combatting ransomware, as expressed in CIRCIA. Lastly, as a policy matter, OFAC's

---

[3] Amy Deen Westbrook, *A Safe Harbor for Ransomware Payments: Protecting Stakeholders, Hardening Targets, and Defending National Security*, 18 N.Y.U. J.L. & BUS. 391, 412 (2022).

[4] STAFF OF S. COMM. ON HOMELAND SEC. & GOVERNMENTAL AFFS., 117TH CONG., USE OF CRYPTOCURRENCY IN RANSOMWARE ATTACKS, AVAILABLE DATA, AND NATIONAL SECURITY CONCERNS 5, 39 n.173 (Comm. Print 2022) [hereinafter SENATE REPORT].

[5] Cyber Incident Reporting for Critical Infrastructure Act of 2022, Pub. L. No. 117-103, §§ 101–03, 2240–46, 136 Stat. 1038, 1038–54 (codified at 6 U.S.C. §§ 101, 665j, 681–681f).

[6] OFAC ADVISORY, *supra* note 1.

threat is problematic in that it incentivizes ransomware victims to cover up, rather than report, information on their attacks. This Comment does not propose a comprehensive solution to curbing the rise of ransomware attacks in America. Rather, it simply argues that OFAC should renounce its policy and defer to the measured judgment of Congress.

This Comment proceeds in three parts. Part I discusses the evolution of ransomware, law enforcement challenges, and the government's response. Part II discusses the origins and evolution of IEEPA, the statute that OFAC claims authority for its policy, and the constitutional limits of the executive's emergency economic powers. Part III argues that OFAC's policy is (1) unconstitutional because it lacks authorization from either an act of Congress or the Constitution, and (2) problematic because it disincentivizes information sharing.

I. Ransomware Evolution, Law Enforcement Challenges, CIRCIA, and OFAC's Policy

To analyze the validity of OFAC's policy, it is first necessary to discuss the background of ransomware regulation in the United States. Section A discusses ransomware's evolution from a niche criminal hobby to a lucrative, multi-billion-dollar industry. Section B then discusses the challenges faced in ransomware law enforcement. Section C discusses CIRCIA and Congress's plan for curbing ransomware attacks through cooperative information sharing. Lastly, Section D discusses the contours of OFAC's strict liability threat for ransomware payments to entities on its SDN List.

A. *The Evolution of Ransomware—From a Cottage Industry to a Major Problem*

Ransomware is a form of malicious computer software ("malware") that infects a computer network, encrypts data, and then demands the victim pay a ransom to decrypt and recover the files or prevent the hacker from distributing or destroying the data.[7] Victims unknowingly download ransomware by opening email attachments, clicking on online advertisements, or visiting infected websites.[8] In many instances, ransomware infections go undetected for months as malicious actors strategically wait for their moment to strike.[9]

---

[7] *See Ransomware 101*, CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY, https://perma.cc/BXT9-KEEW (defining ransomware as a "form of malware designed to encrypt files on a device, rendering any files and the systems that rely on them unusable").

[8] *Ransomware*, FED. BUREAU OF INVESTIGATION, https://perma.cc/SN9R-5NRL.

[9] Jeffrey May, *Ransomware on the Rise*, MICH. BAR J., May 2022, at 30, 30.

The first reported example of a ransomware attack traces back to 1989, when biologist Joseph Popp distributed 20,000 infected floppy disks to AIDS researchers.[10] Popp's malware encrypted computer files, at which time he demanded the victims send $189 each to a P.O. Box in Panama to decrypt the machines.[11] Given the difficulty of payment and the ease of decryption, the attack led to little profit, and Popp was soon arrested in the United Kingdom and charged with blackmail.[12]

From these humble beginnings, ransomware has mutated into a threat that permeates every part of the global economy.[13] While the government and private entities have struggled to compile a comprehensive data set,[14] the available data paints an alarming picture. Since 2016, an average of 4,000 ransomware attacks occur daily in the United States alone.[15] Malicious actors target entities across a broad range of sectors, including healthcare, education, and government (at the federal, state, and local levels).[16] Attackers regularly target small-to-medium-sized businesses: in 2020, 55% of all ransomware attacks hit businesses with less than 100 employees, and 75% hit businesses with under $50 million in revenue.[17] In 2020 alone, nearly 2,500 ransomware attacks were reported to the Federal Bureau of Investigation ("FBI").[18]

Perhaps the most concerning trend in ransomware is the exponential growth in costs. The average ransomware demand jumped from $5,000 in 2018 to roughly $200,000 in 2020.[19] But the true cost of ransomware is more than just the ransom demanded: one report suggested that the cost of operational downtime caused by an attack is nearly fifty times greater than the ransom requested.[20] In other words, the cost of being locked out

---

10 Kaveh Waddell, *The Computer Virus That Haunted Early AIDS Researchers*, THE ATLANTIC (May 10, 2016), https://perma.cc/A954-2EK9.

11 *Id.*

12 *Id.*

13 *See* Westbrook, *supra* note 3, at 404.

14 *See infra* Section I.B for a discussion on the lack of ransomware information sharing.

15 U.S. DEP'T OF JUST. ET AL., HOW TO PROTECT YOUR NETWORKS FROM RANSOMWARE [hereinafter DOJ RANSOMWARE ADVISORY], https://perma.cc/SZ9X-QLAV.

16 *The State of Ransomware in the US: Report and Statistics 2020*, EMSISOFT BLOG (Jan. 18, 2021) [hereinafter EMSISOFT *Report*], https://perma.cc/TT6T-Z69Q (finding that in 2020, ransomware attackers hit at least 560 healthcare facilities, 1,681 educational institutions, and 113 government agencies).

17 *Ransomware Attacks Fracture Between Enterprises and Ransomware-as-a-Service in Q2 as Demands Increase*, COVEWARE (Aug. 3, 2020) [hereinafter COVEWARE *Report*], https://perma.cc/5XMV-47AH.

18 FED. BUREAU OF INVESTIGATION, INTERNET CRIME REPORT 2020 14 (2021) [hereinafter 2020 FBI CRIME REPORT], https://perma.cc/LTA3-EL6R.

19 *The Growing Ransomware Wave*, NAT'L SEC. INST. [hereinafter NSI *Report*], https://perma.cc/23F6-ADQS; COVEWARE *Report*, *supra* note 17.

20 *Datto's Global State of the Channel Ransomware Report*, DATTO [hereinafter DATTO *Report*], https://perma.cc/XLQ4-76Q8; *see also* Jessica Davis, *Ransomware Causes 15 Days of EHR Downtime, as*

of encrypted files is often exponentially more expensive than the ransom demand itself. In total, ransomware cost businesses $20 billion in 2021.[21] By 2031, the average annual cost is expected to reach to $265 billion.[22]

Though the empirical data remains scattered and incomplete, it nevertheless illustrates the magnitude of the problem. Ransomware impacts organizations across all sectors, imposes billions of dollars in costs, and is likely here to stay.

B. *The Challenges of Ransomware Law Enforcement: Identity, Accountability, and Information*

Certain characteristics unique to ransomware have hindered law enforcement efforts and allowed cybercriminals to thrive. First, because cybercriminals demand ransomware payments in the form of cryptocurrency, like Bitcoin, law enforcement often struggles to track the source of attacks.[23] Cryptocurrencies are pseudonymous: while each exchange in cryptocurrency is recorded on a digital ledger, the accounts are tied to digital addresses, rather than to individual names or addresses.[24] To complicate matters further, ransomware attackers typically launder payments through "mixers," where potentially identifiable or tainted funds are mixed in a pool of other funds, thereby increasing the difficulty of tracing funds back to the original source.[25]

Second, ransomware is often used as a tool to further nations' geo-political objectives without triggering economic sanctions. National governments, such as Russia, China, and Iran, have either encouraged or refused to condemn ransomware attacks against organizations from the

---

Payments Avg $111K, TECHTARGET (May 4, 2020), https://perma.cc/22EQ-FK6C; Paul Bischoff, *Ransomware Attacks Cost the US $159.4bn in Downtime Alone in 2021*, COMPARITECH (July 19, 2022), https://perma.cc/H4P5-XS7W.

21 David Braue, *Global Ransomware Damage Costs Predicted to Exceed $265 Billion By 2031*, CYBERCRIME MAG. (June 2, 2022), https://perma.cc/2N9E-X59C.

22 *Id.*

23 James A. Sherer, Melinda L. McLellan, Emily R. Fedeles & Nichole L. Sterling*, Ransomware – Practical and Legal Considerations for Confronting the New Economic Engine of the Dark Web*, 23 RICH. J.L. & TECH. 1, 38 (2017).

24 Westbrook, *supra* note 3, at 415–17 ("[C]ryptocurrency transfers—including ransom payments—are generally difficult to connect with a particular person . . . .").

25 *The Wild World of Crypto Ransomware Payments,* FIN. EXECS. INT'L DAILY (Oct. 25, 2021), https://perma.cc/C64N-83MK. The FBI's Recovery Asset Team ("RAT"), which functions as a "liaison between law enforcement and financial institutions," has reported success in freezing assets for reporting entities. FED. BUREAU OF INVESTIGATION, INTERNET CRIME REPORT 2022 9–10 (2023) [hereinafter 2022 FBI REPORT], https://perma.cc/8JTU-UKK5. Since its creation in 2018, RAT reports a 73% success rate, freezing $433.30 million out of $590.62 million in fraudulent transfers. *Id.*

United States and other rival countries.[26] Experts recognize that the connection between national governments and cybercriminals is obscure by design: states establish ambiguous relationships with cybercriminals to create plausible deniability as to awareness of their criminal activities.[27] For example, when asked about Russian cyber interference in the 2016 U.S. presidential election, Russian Prime Minister Vladimir Putin stated, "If they did not break Russian law, there is nothing to prosecute them for in Russia."[28]

Third, perhaps most pertinent, the lack of information sharing between victims and the government hampers ransomware regulation. A 2021 investigative report by the Senate Committee on Homeland Security and Government Affairs highlighted the need for increased information sharing, noting that only about 25% of ransomware attacks are reported to the government.[29] With more information sharing, "the federal government will be in a better position to assist existing and potential cybercrime victims with prevention, detection, mitigation, and recovery" and "facilitate[] more efficient investigation and prosecution of illicit actors."[30] But without three-quarters of the available data, the effectiveness of the government's enforcement tools is blunted and the development of effective solutions is inhibited.[31] The significance of this data shortage is obvious: with only a fraction of the available data on ransomware attacks, U.S. law enforcement fights an enemy in the dark.

The lack of ransomware reporting may reflect the victims' risk landscape: if an attack were to go public, a victim organization may face significant reputational harm, regulatory fines, and civil litigation. As a

---

[26] Westbrook, *supra* note 3, at 410–12; Emily Flitter & David Yaffe-Bellany, *Russia Could Use Cryptocurrency to Blunt the Force of U.S. Sanctions,* N.Y. TIMES (Feb. 23, 2022), https://perma.cc/7WWB-2MKC.

[27] *See, e.g.*, Erica D. Lonergan, *Cyber Proxies in the Ukraine Conflict: Implications for International Norms*, COUNCIL ON FOREIGN REL. (Mar. 21, 2022), https://perma.cc/MXJ4-2LKZ.

[28] Isabelle Khurshudyan & Loveday Morris, *Ransomware's Suspected Russian Roots Point to a Long Detente Between the Kremlin and Hackers*, WASH. POST (June 12, 2021), https://perma.cc/GA8V-THVD ("[Russian cybercriminals] explicitly say there's no going after Russian targets, . . . [a]nd that allows them to operate with impunity. . . . They are not operating at the behest of Russia, but they're operating with the tacit acknowledgement of Russia.").

[29] SENATE REPORT, *supra* note 4, at 5.

[30] *Id.* at 3.

[31] *Id.* at 4. The FBI has publicly acknowledged its limited data set and the need for increased information sharing. In its 2022 Internet Crime Report, the FBI stated,

> [I]t has been challenging for the FBI to ascertain the true number of ransomware victims as many infections go unreported to law enforcement. By reporting the incident, the FBI may be able to provide information on decryption, recover stolen data, [seize/recover] ransom payments, and gain insight on adversary tactics. Ultimately, the information you provide will lead us to bring the perpetrators to justice.

2022 FBI REPORT, *supra* note 25, at 13.

result, many victims, like the lawyer in the opening hypothetical, find that covering up an attack is the most prudent decision for their organization.

C. *CIRCIA: Congress Prescribes Mandatory Reporting with Liability Protections*

Federal agencies have pushed for increased information sharing between the private and public sectors to address the persistent ransomware threat. The federal government has historically relied on voluntarily-reported information and a patchwork of laws, regulations, and guidance to map out the ransomware threat landscape.[32] As discussed above, these methods have proven ineffective. For example, experts describe the FBI's ransomware dataset as "a subset of a subset of data," with figures that are "incredibly low" and "inconsistent."[33] As suggested by one expert, the incomplete dataset on ransomware can be explained by a "lack of reporting requirements and incentives [to cooperate]."[34]

In 2021, several bills aimed at increasing ransomware information sharing were introduced and considered in Congress.[35] Ultimately, Congress passed the Cyber Incident Reporting for Critical Infrastructure Act of 2022, which was signed into law by President Biden that March.[36] CIRCIA required the director of the Cybersecurity and Infrastructure Agency ("CISA") to publish proposed rules for implementing the statute's reporting requirements by March 2024 and set the deadline for the final rule at eighteen months from the publishing of the proposed rules.[37]

Under CIRCIA, organizations in critical infrastructure sectors must report cyber incidents to CISA within seventy-two hours from the time they "reasonably believe" the incident occurred.[38] If a ransom payment is made after a ransomware attack, CIRCIA requires the entity to report to CISA within twenty-four hours.[39]

---

32 SENATE REPORT, *supra* note 4, at 35 (noting that while the DOJ, SEC, and FinCEN each collect data on ransomware, no dataset is accessible across government agencies).

33 Alexander Culafi, *FBI IC3 Report's Ransomware Numbers Are Low, Experts Say*, TECHTARGET (Mar. 18, 2021), https://perma.cc/Z7GR-BB4Y.

34 SENATE REPORT, *supra* note 4, at 40.

35 CHRIS JAIKARAN, CONG. RSCH. SERV., R46944, CYBERSECURITY: COMPARISON OF SELECTED CYBER INCIDENT REPORTING BILLS—IN BRIEF 1 (2021) [hereinafter PROPOSED INCIDENT REPORTING BILLS] (comparing four cyber incident reporting bills from the first session of the 117th Congress: the Cyber Incident Reporting for Critical Infrastructure Act of 2021 (H.R. 5440), the Cyber Incident Notification Act of 2021 (S. 2407), the Cyber Incident Reporting Act of 2021 (S. 2875), and the Ransom Disclosure Act (S. 2943)).

36 CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY, CYBER INCIDENT REPORTING FOR CRITICAL INFRASTRUCTURE ACT OF 2022 (CIRCIA) FACT SHEET 1 (2022), https://perma.cc/2MNF-B344.

37 Cyber Incident Reporting for Critical Infrastructure Act of 2022, Pub. L. No. 117-103, § 2242(b), 136 Stat. 1038, 1044 (codified at 6 U.S.C. § 681b).

38 *Id.* § 2242(a)(1).

39 *Id.* § 2242(a)(2).

The reporting requirements in CIRCIA apply only to what the statute defines as "covered entities."[40] Covered entities are organizations in sixteen critical infrastructure sectors "vital to . . . the Nation's safety, prosperity, and well-being,"[41] including organizations in the communications, energy, financial services, and transportation systems sectors.[42] CIRCIA encourages but does not require non-covered entities to report cyber incidents as well.

CIRCIA provides comprehensive liability protections for reporting entities, whether the information is reported mandatorily or voluntarily. For one, the statute provides that the government will treat reported information as "the commercial, financial, and proprietary information of the covered entity."[43] In other words, the government will not make the information provided publicly available, nor allow it to be used as the basis of civil litigation. In addition, CIRCIA prohibits federal, state, and local governments from pursuing enforcement actions based on information in reports.[44] In the context of ransomware, this clause prohibits the government at all levels from prosecuting reporting entities for ransomware payments based on reported information.[45] By prohibiting the use of reported information in litigation and government enforcement actions, CIRCIA significantly reduces the risks faced by ransomware victims in sharing information with the government.

CIRCIA's explicit liability protections suggest that, after considering and debating various solutions to curb the ransomware problem,[46] Congress determined that the best defense against today's ransomware threat is to provide victims with liability *protection*, not liability *imposition*. CIRCIA's combination of reporting obligations and liability protections ensures greater governmental awareness of ransomware attacks and incentivizes cooperation by lowering the liability risk for reporting entities. With these protections, the government will gain better access to the most important tool in curbing ransomware: information. In sum, CIRCIA illustrates that, with respect to ransomware payments, Congress has decided that the "carrot" is more effective than the "stick."

---

40 *Id.* § 2240 (codified at 6 U.S.C. § 681). CIRCIA borrows the definition of "covered entities" from Presidential Policy Directive 21, though it requires the Director of CISA to promulgate a specific definition by the final rule. *Id.*

41 *Id.*; Press Release, Off. of the Press Sec'y, The White House, Presidential Policy Directive—Critical Infrastructure Security and Resilience (Feb. 12, 2013) [hereinafter Presidential Policy Directive], https://perma.cc/2PKM-5AP8.

42 Presidential Policy Directive, *supra* note 41. Chemical, Commercial Facilities, Critical Manufacturing, Dams, Defense Industrial Base, Emergency Services, Food and Agriculture, Governmental Facilities, Information Technology, Nuclear, and Water and Wastewater Systems are also designated as critical infrastructure sectors. *Id.*

43 Cyber Incident Reporting for Critical Infrastructure Act of 2022 § 2245(b)(1).

44 *Id.* § 2245(a)(5)(A).

45 *Id.*

46 PROPOSED INCIDENT REPORTING BILLS, *supra* note 35, at 1.

D. *OFAC's Ransomware Policy*

As opposed to CIRCIA's cooperative information-sharing framework, OFAC has opted to threaten victims of ransomware attacks with strict liability civil penalties for payments to persons on its SDN List. Subsection 1 discusses OFAC's SDN List designation process and Subsection 2 outlines OFAC's ransomware policy.

1. The SDN List Designation Process

OFAC's SDN List is comprised of individuals and entities located in, controlled by, or acting on behalf of, several targeted countries, like North Korea, Iran, Syria, and Cuba.[47] The SDN List also includes non-governmental actors, such as terrorist organizations and narcotics traffickers.[48] Once designated to the SDN List, OFAC blocks the entity's assets and generally prohibits U.S. persons from dealing with them.[49]

OFAC has designated several malicious cyber actors under its cyber-related sanctions program and other sanctions programs.[50] For example, in December 2016, OFAC designated Evgeniy Mikhailovich Bogachev, the developer of a ransomware strain known as "Cryptolocker" that infected over 234,000 computers.[51] In December 2019, OFAC designated Evil Corp, a Russia-based cybercriminal organization that launched ransomware attacks against hundreds of financial institutions across forty countries.[52] OFAC has extended the SDN List to include cryptocurrency exchanges: in September 2021, OFAC designated SUEX OTC, S.R.O. for its part in facilitating financial transactions for ransomware attackers.[53]

In the context of cybercrime, OFAC's designation process has faced challenges. Because cryptocurrencies allow ransomware attackers to retain their anonymity, OFAC can designate only the attackers' digital currency addresses ("cryptocurrency wallets") to its SDN List.[54] Ransomware attackers, once designated to the SDN List, routinely re-

---

47 OFF. OF FOREIGN ASSETS CONTROL, U.S. DEP'T OF THE TREASURY, SPECIALLY DESIGNATED NATIONALS AND BLOCKED PERSONS LIST (SDN) HUMAN READABLE LISTS (Jan. 6, 2023), https://perma.cc/U4ZN-98AQ; OFF. OF FOREIGN ASSETS CONTROL, U.S. DEP'T OF THE TREASURY, SANCTIONS PROGRAMS AND COUNTRY INFORMATION, https://perma.cc/BD2C-BH46.

48 OFF. OF FOREIGN ASSETS CONTROL, U.S. DEP'T OF THE TREASURY, SANCTIONS PROGRAMS AND COUNTRY INFORMATION, https://perma.cc/BD2C-BH46.

49 *Id.*

50 OFAC ADVISORY, *supra* note 1, at 2.

51 *Id.*

52 *Id.* at 3.

53 *Id.*

54 SENATE REPORT, *supra* note 4, at 45.

brand their organizations and create new cryptocurrency wallets.[55] For example, shortly after OFAC designated Evil Corp, several experts suspected that the group simply re-branded to "Babuk" to shirk OFAC sanctions.[56] Thus, the wallets listed on OFAC's SDN List are often either outdated or inaccurate.[57]

2. OFAC's Ransomware Payment Policy and Enforcement Framework

In October 2020 and September 2021, OFAC released and updated an advisory claiming the authority to impose strict liability civil penalties on ransomware victims for payments to entities on its SDN List.[58] The policy states that ransomware payments may "enable criminals and adversaries with a sanctions nexus to profit and advance their illicit aims" or "fund activities adverse to the national security and foreign policy objectives of the United States."[59] OFAC claims the authority to impose these strict liability penalties under the International Emergency Economic Powers Act.[60]

When OFAC determines the occurrence of a violation, it typically issues a pre-penalty notice and provides an opportunity for a written response.[61] Ultimately, the director of OFAC retains the discretion to determine whether to impose a penalty and the amount of that penalty, limited only by OFAC's "Enforcement Guidelines."[62] OFAC recognizes two significant mitigating factors for ransomware payments. First, OFAC will consider "the existence, nature, and adequacy of a sanctions compliance program."[63] If a victim takes "meaningful steps . . . to reduce the risk of extortion by a sanction actor through improving cybersecurity practices," it may mitigate the severity of OFAC's enforcement response.[64] Second, OFAC will consider "the nature and extent of a [victim's] cooperation with

---

55 *Id.*; *see, e.g.*, Lawrence Abrams, *Conti Ransomware Shuts Down Operation, Rebrands Into Smaller Units*, BLEEPINGCOMPUTER (May 19, 2022), https://perma.cc/2JFP-FHD8.

56 Phil Muncaster, *Evil Corp Rebrands Ransomware to Escape Sanctions*, INFOSECURITY MAG. (June 8, 2021), https://perma.cc/L5RQ-CJWN.

57 SENATE REPORT, *supra* note 4, at 45.

58 OFAC ADVISORY, *supra* note 1, at 4.

59 *Id.* at 3. OFAC's policy marks a departure from the FBI's position on ransomware payments. In 2019, the FBI released guidance stating that, although it "does not advocate paying a ransom," "the FBI understands that when businesses are faced with an inability to function, executives will evaluate all options to protect their shareholders, employees, and customers." FED. BUREAU OF INVESTIGATION, FBI PUBLIC SERVICE ANNOUNCEMENT, ALERT NO. I-100219-PSA, HIGH-IMPACT RANSOMWARE ATTACKS THREATEN U.S. BUSINESS AND ORGANIZATIONS, (2019), https://perma.cc/C8HR-FJKF.

60 OFAC ADVISORY, *supra* note 1, at 3.

61 31 C.F.R. pt. 501, app. A § V(A) (2023).

62 *Id.* §§ II(A), III.

63 OFAC ADVISORY, *supra* note 1, at 4.

64 *Id.*

OFAC, law enforcement, and other relevant agencies, including whether an apparent violation of U.S. sanctions is voluntarily self-disclosed."[65] If a victim voluntarily discloses information and cooperates fully with law enforcement, OFAC suggests it would impose only a mild penalty.[66]

As opposed to CIRCIA's cooperative approach, which provides comprehensive liability protections to victims, OFAC's policy starts with a presumption of liability for payments to attackers who happen to be on the agency's SDN List.[67] This liability can be mitigated only if OFAC's director finds that the victim had adequate cybersecurity hygiene practices and cooperated sufficiently with law enforcement.

OFAC's policy takes the opposite approach of CIRCIA in incentivizing victims to report. Under CIRCIA, the government aims to incentivize information sharing by minimizing the risk of reporting.[68] If a victim organization fulfills its reporting obligations, it is immune from certain risks, including government enforcement and civil litigation based on the reported information.[69] OFAC, on the other hand, attempts to incentivize information sharing by increasing the risk of not reporting. If OFAC finds that the attacker is on the agency's SDN List, it may penalize the victim at its discretion.[70] This risk is heightened even more by the difficulty or impossibility for victims to identify their attackers.[71] By threatening the victims of ransomware attacks with strict liability civil penalties, OFAC has opted for the "stick," rather than the "carrot," to curb ransomware attacks.

II. The Origins of IEEPA and Judicial Interpretation of Executive Emergency Economic Powers

To determine the legality of OFAC's threat of strict liability civil penalties for ransomware payments, it is helpful to examine the source from which OFAC claims this broad authority—the International Emergency Economic Powers Act. IEEPA, as currently amended, provides that the president may "investigate, regulate, or prohibit (1) any transactions in foreign exchange . . . and (2) the importing or exporting of currencies or securities."[72] The president may exercise these powers only

---

65 *Id.* at 5.

66 *Id.*

67 *Id.* at 4.

68 Cyber Incident Reporting for Critical Infrastructure of 2022, Pub. L. No. 117-103, §§ 2245(a)(5)(A), (a)(5)(c), 136 Stat. 1038, 1052–53 (codified at 6 U.S.C. § 681e).

69 *Id.* § 2245(c).

70 OFAC ADVISORY, *supra* note 1, at 3–4.

71 Sherer et al., *supra* note 23, at 19–20.

72 50 U.S.C. § 1702(a)(1)(A).

"to deal with any unusual and extraordinary threat, which has its source in whole or substantial part outside the United States."[73]

Section A discusses IEEPA's predecessor, the Trading with the Enemy Act of 1917 ("TWEA"), and the problems that Congress intended for IEEPA to remedy. Section B outlines the substantive limitations under IEEPA. Lastly, Section C discusses the courts' interpretation of the executive's emergency power and IEEPA.

A. *TWEA: From a Limited Wartime Statute to a Source of Vast Executive Power*

The origins of the International Economic Powers Act trace back to 1917 and the Trading with the Enemy Act. Congress passed TWEA to regulate private international transactions with enemy powers following the United States' entry into World War I.[74] Section 5(b) of TWEA, as originally enacted, states:

> [T]he President may investigate, regulate, or prohibit, under such rules and regulations as he may prescribe . . . any transaction in foreign exchange . . . between the United States and any foreign country, whether enemy, ally of enemy, or otherwise, or between residents of one or more foreign countries, by any person within the United States.[75]

While the statute was originally intended for use during the war, Congress amended Section 5(b) of TWEA in 1933 for peacetime application: "During time of war *or during any other period of national emergency declared by the President* . . . ."[76] Following this amendment, presidents utilized TWEA to address numerous challenges associated with the Great Depression, World War II, and the Cold War.[77] TWEA functioned as a "convenient statutory basis for vast *peacetime* exercises of exceptional economic authority which its authors clearly did not have in mind."[78]

By the mid-1970s, Congress began pushing back on executive discretion after a series of scandals involving the executive branch.[79] The Senate formed the bipartisan "Senate Special Committee on the Termination of the National Emergency" in 1976 to re-evaluate

---

73 *Id.* § 1701(a).

74 Benjamin A. Coates, *The Secret Life of Statutes: A Century of the Trading with the Enemy Act*, 1 MOD. AM. HIST. 151, 152 (2018).

75 Trading with the Enemy Act, Pub. L. No. 65-91, § 5(b), 40 Stat. 411, 415 (1917) (codified as amended at 50 U.S.C. § 4305(b)).

76 Emergency Banking Relief Act, ch. 1, sec. 2, § 5(b), 48 Stat. 1, 1 (1933) (emphasis added).

77 CHRISTOPHER A. CASEY, IAN F. FERGUSSON, DIANNE E. RENNACK & JENNIFER K. ELSEA, CONG. RSCH. SERV., R45618, THE INTERNATIONAL EMERGENCY ECONOMIC POWERS ACT: ORIGINS, EVOLUTION, AND USE 4–6 (2020) [hereinafter IEEPA ORIGINS, EVOLUTION, AND USE] (outlining the expansion of executive power under TWEA following the 1933 amendment).

78 William E. Sheuerman, *The Economic State of Emergency*, 21 CARDOZO L. REV. 1869, 1878 (2000).

79 IEEPA ORIGINS, EVOLUTION, AND USE, *supra* note 77, at 6–8.

delegations of emergency authority to the president.[80] The Committee found that the United States had technically been in a state of emergency since March 9, 1933.[81] During this period, over 740 emergency statutes delegated authority, usually limited to Congress, to the executive's discretionary powers "which affect[ed] the lives of American citizens in a host of all-encompassing ways."[82] The Committee's central concern focused on "whether it was possible for [the American] democratic government . . . to exist under its present Constitution and system of three separate branches equal in power under a continued state of emergency."[83]

Concern over the executive's broad emergency powers was not limited to the Senate. In 1977, during the House markup of a bill revising TWEA, Representative Jonathan Bingham, Chairperson of the House International Relations Committee's Subcommittee on Economic Policy, described TWEA as conferring on the president "dictatorial powers that he could have used without any restraint by Congress."[84]

The House raised four primary concerns with TWEA: (1) it required no consultation or reports to Congress with regard to the use of powers or the declaration of a national emergency; (2) it set no time limits on a state of emergency and no mechanism for congressional review; (3) it stated no limits on the scope of TWEA's economic powers and the circumstances under which such authority could be used; and (4) the actions taken under the authority of TWEA rarely related to the circumstances of the declared national emergency.[85] Professor Harold G. Maier summarized the main criticisms of TWEA when testifying before the House Committee on International Relations: "Section 5(b)'s effect is no longer confined to 'emergency situations' in the sense of existing imminent danger. [Congress's routine retroactive approvals] of broad executive interpretations of the scope of power which it confers has converted the section into a general grant of legislative authority to the President . . . ."[86]

---

[80] SUBCOMM. ON INT'L TRADE AND COM. OF THE H. COMM. ON INT'L RELS., 94TH CONG., TRADING WITH THE ENEMY: LEGISLATIVE AND EXECUTIVE DOCUMENTS CONCERNING REGULATION OF INTERNATIONAL TRANSACTIONS IN TIME OF DECLARED NATIONAL EMERGENCY (Comm. Print 1976) [hereinafter TWEA REPORT].

[81] Harold Relyea, A Brief History of Emergency Powers in the United States (July 1974) (unnumbered working paper) (on file with the *George Mason Law Review*).

[82] *Id.*

[83] TWEA REPORT, *supra* note 80.

[84] H. COMM. ON INT'L RELS., 95TH CONG., REVISION OF THE TRADING WITH THE ENEMY ACT: MARKUP BEFORE THE COMMITTEE ON INTERNATIONAL RELATIONS 5 (Comm. Print 1977).

[85] H. COMM. ON INT'L RELS., 95TH CONG., TRADING WITH THE ENEMY ACT REFORM LEGISLATION, H.R. REP. NO. 95-459, at 10 (1977) (Conf. Rep.).

[86] *Id.* at 9.

B. *IEEPA: A Statutory Limitation on the Executive's Economic Emergency Powers*

Congress moved to remedy the expansion of executive power under TWEA in two steps. In step one, Congress enacted the National Emergencies Act of 1976 ("NEA"),[87] which placed new restrictions on both the declaration and duration of new states of emergency.[88] The statute further checked the executive's emergency powers by (1) requiring that the president report to Congress whenever they declare a new state of emergency, and (2) allowing Congress to terminate states of emergency by concurrent resolution ("legislative veto").[89]

In step two, Congress amended TWEA to apply only "in time of war," as the original drafters intended.[90] Congress then wrote IEEPA to confer emergency powers "both more limited in scope than those of Section 5(b) [of TWEA] and subject to various procedural limitations, including those of [NEA]."[91] The Report of the House Committee on International Relations explained the nature of an "emergency" under IEEPA:

> The main [substantive restriction under IEEPA] stems from a recognition that emergencies are by their nature *rare* and *brief*, and are *not to be equated with normal, ongoing problems*. . . . The emergency should be terminated in a timely manner when the factual state of emergency is over and not continued in effect for use in other circumstances. A state of national emergency should not be a normal state of affairs.[92]

Against this backdrop, Congress drafted IEEPA to confer power in limited situations:

> [The powers under IEEPA] may be exercised to deal with any *unusual* and *extraordinary* threat, which has its source in whole or substantial part outside the United States, to the national security, foreign policy, or economy of the United States, if the President declares a national emergency with respect to such threat.[93]

IEEPA contains two substantive restrictions to protect against the issues that had arisen under its predecessor. First, the powers under IEEPA are limited by its text: they may be used only to deal with "unusual and extraordinary" foreign threats to the national security, foreign policy, and

---

87 Pub. L. No. 94-412, 90 Stat. 1255 (1976) (codified as amended at 50 U.S.C. § 1601).

88 *Id.* §§ 201, 202 (codified as amended at 50 U.S.C. §§ 1621, 1622).

89 *Id.* The NEA's concurrent resolution provision, which required only a simple majority in either house to terminate a state of emergency, was later abrogated by the Supreme Court's decision in *INS v. Chadha*, which held legislative vetoes unconstitutional. 462 U.S. 919, 959 (1983). In response, Congress amended the NEA to change "concurrent" resolution to "joint" resolution. Foreign Relations Authorization Act, Fiscal Years 1986 and 1987, Pub. L. No. 99-93, sec. 801, § 202(2), 99 Stat. 405, 448 (1985).

90 Act of Dec. 28, 1977, Pub L. No. 95-223, sec. 101, § 5(b)(1), 91 Stat. 1625 (codified as amended at 50 U.S.C. § 4305).

91 H. COMM. ON INT'L RELS., 95TH CONG., TRADING WITH THE ENEMY ACT REFORM LEGISLATION, H.R. REP. No. 95-459, at 2 (1977) (Conf. Rep.).

92 *Id.* at 10 (emphasis added).

93 50 U.S.C. § 1701(a) (emphasis added).

economy of the United States.[94] Second, the powers are restricted by the "nature" of the term "emergencies." IEEPA is not "a general grant of legislative authority to the president" to deal with "normal ongoing problems," but a limited grant of authority for "unusual and extraordinary" foreign threats.

C. *Judicial Limits on the Executive's Emergency Powers*

While the Supreme Court has rarely pushed back on the executive's use of emergency powers, it has not suggested that such power is unlimited.[95] The Court addressed the issue in *Youngstown Sheet & Tube Co. v. Sawyer*.[96] During the Korean conflict, a labor dispute broke out between steel mill owners and employees.[97] Fearing that a stoppage of steel production would result in a national catastrophe, President Truman ordered the Secretary of Commerce to take possession of the steel mills to continue their operation.[98] Shortly before this emergency, Congress passed the Taft-Hartley Act, which prescribed a more cooperative method for resolving labor disputes.[99] Notably, Congress refused to adopt an amendment that authorized the seizure of factories during emergencies.[100] The majority held that the president's exercise of this emergency power was unconstitutional as its source could not be traced to either an act of Congress or the Constitution.[101]

In a concurring opinion, Justice Robert Jackson famously laid out a three-category framework for analyzing the constitutionality of executive action. In the first category, the president acts pursuant to an express or implied grant of Congress.[102] Presidential authority is at its "maximum" in these circumstances.[103] In the second, the president acts in the absence of either a congressional grant or denial of authority.[104] Here, the president's authority is in a "zone of twilight" where congressional "inertia, indifference, or acquiescence" may invite presidential action.[105] Lastly, in

---

94 *Id.*

95 *See* Youngstown Sheet & Tube Co. v. Sawyer, 343 U.S. 579, 585 (1952) ("The President's power . . . must stem either from an act of Congress or from the Constitution itself."); *see also id.* at 652 (Jackson, J., concurring) ("[E]mergency powers are consistent with free government only when their control is lodged elsewhere than in the Executive who exercises them.").

96 *Id.* at 582 (majority opinion).

97 *Id.*

98 *Id.* at 583.

99 *Id*. at 586; Labor Management Relations Act, 29 U.S.C. §§ 141, 171–80.

100 *Youngstown*, 343 U.S. at 586; 93 CONG. REC. 3637–45 (1947).

101 *Youngstown*, 343 U.S. at 589.

102 *Id.* at 635–37 (Jackson, J., concurring).

103 *Id.* at 635.

104 *Id.* at 637.

105 *Id.*

the third category, the president's actions are incompatible with the express or implied will of Congress. Presidential authority is at its "lowest ebb" in these situations as they can rely "only upon [their] own constitutional powers minus any constitutional powers of Congress over the matter."[106]

Justice Jackson ultimately concluded that the president's actions fell within the third category as Congress neither authorized the seizure nor "left seizure of private property an open field."[107] Accordingly, the president could not claim that his actions were "necessitated or invited by the failure of Congress to legislate upon the occasions."[108]

In *Dames & Moore v. Regan*,[109] the Court cited the *Youngstown* framework as it discussed the scope of the president's powers under IEEPA.[110] There, the petitioners challenged a series of actions taken by President Carter to implement the Algiers Accords, which the president entered into to end the hostage crisis in Iran.[111] Among other things, the president ordered the resolution of all claims against the Iranian government in U.S. courts.[112] IEEPA explicitly authorized most of the president's actions, including the nullification of prejudgment attachments and the transfer of property to Iran.[113] However, the Court held that the terms of the IEEPA did not authorize the president's suspension of claims.[114] As an act of Congress also did not bar the action, the Court examined the constitutionality under Justice Jackson's "zone of twilight" category:

> [T]he enactment of legislation closely related to the question of the President's authority in a particular case which evinces legislative intent to accord the President broad discretion may be considered to invite measures of independent presidential responsibility. At least this is so where there *is no contrary indication of legislative intent and when, as here, there is a history of congressional acquiescence in conduct of the sort engaged in by the President*.[115]

The Court looked to a long history of "congressional acquiescence" in the president's exercise of claim settlement authority and determined that it had "implicitly approved" of the practice.[116] The "general tenor" of Congress's legislation in the areas of emergencies and hostage negotiations evidenced Congress's acquiescence to the president's

---

106 *Id.*

107 *Youngstown*, 343 U.S. at 639–40.

108 *Id.*

109 453 U.S. 654 (1981).

110 *Id.* at 668–69.

111 *Id.* at 662–68.

112 *Id.* at 666; Exec. Order No. 12,283, 46 Fed. Reg. 7927, 7927 (Jan. 19, 1981).

113 *Dames*, 453 U.S. at 674.

114 *Id.* at 675.

115 *Id.* at 678–79 (emphasis added) (internal citations omitted).

116 *Id.* at 679–80.

authority to issue claim settlement agreements.[117] The Court also found persuasive that Congress drafted legislation on the assumption that the president had the authority to issue such agreements.[118] As the Court explained, a "long-continued practice, known to and acquiesced in by Congress, [raises] a presumption that the [action] had been [taken] in pursuance of its consent."[119] On these case-specific considerations, the Court held that President Carter's claim settlement order was a proper exercise of executive power.[120]

Dames & Moore illustrates the Court's approach in determining the constitutionality of the executive's emergency powers under Justice Jackson's "zone of twilight" category: if a challenged action aligns with a history of "congressional acquiescence" to the president's exercise of such power, it "may be treated as a gloss on 'Executive Power' vested in the President by § 1 of Art. II."[121] Absent such congressional acquiescence, the Court may not afford executive action with a presumption of constitutionality.

III. The Legal and Policy Concerns with OFAC's Ransomware Policy

OFAC's threat of strict liability civil penalties is unlawful and problematic. Section A argues that OFAC's policy is unconstitutional because neither a statute nor the Constitution authorized it. Section B argues that OFAC's policy is problematic because it encourages victims to conceal, rather than share, information on ransomware attacks. For these reasons, OFAC should renounce its policy and defer to Congress's measured judgment and the CIRCIA framework.

---

117 *Id.* at 677–78. The president has broad discretion in matters of hostage settlements and emergencies, respectively. *See* 22 U.S.C. § 1732; 50 U.S.C. § 1702(a)(1). While neither statute specifically authorized the president to issue claim settlements, the Court determined that both statutes were "highly relevant in the looser sense of indicating congressional acceptance of a broad scope for executive action in circumstances such as those presented in this case." *Dames*, 453 U.S. at 677.

118 *Dames*, 453 U.S. at 680–81. For example, the International Claims Settlement Act of 1949 created a procedure for implementing future claim settlement agreements. International Claims Settlement Act of 1949, ch. 54, 64 Stat. 12 (1950) (codified as amended at 22 U.S.C. §§ 1621–27). The Court determined that the statute signified Congress's "stamp of approval on such agreements." *Dames*, 453 U.S. at 680.

119 *Dames*, 453 U.S. at 686 (second and third alteration in original) (quoting United States v. Midwest Oil Co., 263 U.S. 459, 474 (1915)).

120 *Id.*

121 *Id.* (quoting Youngstown Sheet & Tube Co. v. Sawyer, 343 U.S. 579, 610–11 (1952) (Frankfurter, J., concurring)).

A. *The Legal Concerns: OFAC's Policy Is Unconstitutional Because It Is Not Authorized by an Act of Congress or the Constitution.*

Because OFAC's policy cannot trace its power to a statute or the Constitution, it is unconstitutional. First, Subsection 1 argues that OFAC's policy is not authorized by the IEEPA because it conflicts with the statute's text, legislative intent, and central purpose. Subsection 2 argues that OFAC's policy violates separation-of-powers principles as it conflicts with Congress's mechanism for curbing ransomware attacks and does not otherwise fall within the "executive power."

1. OFAC's Policy Is Not Authorized by IEEPA Because It Conflicts with the Statute's Text, Legislative Intent, and Central Purpose

OFAC's ransomware policy is not authorized by IEEPA, the statute in which it claims authority. First, ransomware does not fit within the statute's text because ransomware attacks are neither unusual nor extraordinary. Second, OFAC's policy is inconsistent with the drafters' understanding of "emergency" as ransomware attacks are a normal, ongoing problem rather than a rare and brief threat. Lastly, interpreting IEEPA broadly enough to authorize OFAC's policy would undermine the statute's central purpose of limiting the executive's emergency powers.

OFAC's policy falls outside the scope of IEEPA's text. The statute's broad powers are limited by Section 1701: "[The powers under the IEEPA] may be exercised to deal with any *unusual* and *extraordinary threat*, which has its source in whole or substantial part outside the United States, to the national security, foreign policy, or economy of the United States."[122] But ransomware attacks are neither unusual nor extraordinary. While, in the days of Joseph Popp,[123] it may have been a niche criminal activity, ransomware is now a part of daily life for many Americans. In the United States alone, an average of 4,000 ransomware attacks occur daily.[124] Malicious actors regularly target organizations of all sizes and across all sectors.[125] According to the FBI, whose dataset experts describe as a "subset of a subset" with figures that are "incredibly low,"[126] nearly 2,500 businesses fell victim to ransomware attacks in 2020 alone.[127] As the ransomware threat is far from unusual or extraordinary, OFAC's policy is far from the scope of the IEEPA.

---

122 50 U.S.C. § 1701 (emphasis added).

123 *See* Waddell, *supra* note 10.

124 DOJ RANSOMWARE ADVISORY, *supra* note 15, at 2.

125 *See* EMSISOFT *Report*, *supra* note 16; COVEWARE *Report*, *supra* note 17.

126 Culafi, *supra* note 33.

127 2020 FBI CRIME REPORT, *supra* note 18, at 3.

Given the magnitude of costs associated with ransomware attacks,[128] one could argue that in the modern economy, the threat of ransomware is "unusual and extraordinary." But this interpretation would lead to a TWEA-like expansion of executive power. As discussed in Part I, Section B, the proliferation of ransomware attacks (and therefore, the rise in ransomware costs) is largely due to the government's failure to identify bad actors, hold such actors accountable, and incentivize victims to cooperate. If such challenges qualify as "unusual and extraordinary," the executive could assume legislative authority whenever it struggled to enforce the law. The magnitude of costs represents a need for legislation to aid law enforcement efforts, not "an unusual and extraordinary threat" triggering IEEPA's vast powers.

OFAC's policy also contradicts the IEEPA drafters' understanding of "emergency." As explained by the House Committee on International Relations, the main substantive restriction under IEEPA "stems from a recognition that emergencies are by their nature *rare* and *brief*, and are *not to be equated with normal ongoing problems*."[129]

Ransomware attacks are now a normal ongoing problem. First, given the frequency of attacks and breadth of targets, it cannot be said that ransomware attacks are rare. It would strain the meaning of the word itself to suggest that an event occurring over 4,000 times daily and impacting roughly 2,500 businesses yearly qualifies as "rare."[130] Second, ransomware attacks are not a "brief" issue expected to be resolved anytime in the near future. To the contrary, experts expect that the annual cost of ransomware will increase tenfold over the next ten years, growing from $20 billion in 2021 to $265 billion in 2031.[131] Nothing in the available data suggests that ransomware attacks fit within this understanding of an emergency.

On top of conflicting with IEEPA's terms and legislative intent, OFAC's policy undermines the statute's central purpose: reining in executive emergency power. To interpret IEEPA broadly enough to authorize OFAC's policy would ignore Congress's concerns and revive the issues that arose under its predecessor, TWEA.

The purpose of IEEPA informs the scope of its powers. TWEA, a statute intended for use during wartime, was later amended for use during peacetime.[132] Over the next half century, the statute devolved into a "general grant of legislative authority to the President"[133] and conferred "dictatorial powers that [the President] could have used without any

---

128 *See* NSI *Report*, *supra* note 19.

129 IEEPA ORIGINS, EVOLUTION, AND USE, *supra* note 77, at 11 (emphasis added).

130 *See* DOJ RANSOMWARE ADVISORY, *supra* note 15; 2020 FBI CRIME REPORT, *supra* note 18, at 14.

131 Braue, *supra* note 21.

132 Act of Mar. 9, 1933, ch. 1, sec. 2, § 5(b), 48 Stat. 1.

133 H. COMM. ON INT'L RELS., 95TH CONG., TRADING WITH THE ENEMY ACT REFORM LEGISLATION, H.R. REP. No. 95-459, at 9 (1977) (Conf. Rep.).

restraint by Congress."[134] Among the TWEA revisionists' primary concerns was its failure to state limits on the scope of its economic powers and the circumstances dictating their use.[135] To address these issues, Congress drafted the IEEPA to confer powers "more limited in scope than those in Section 5(b) [of TWEA] and subject to various procedural limitations."[136]

Interpreting IEEPA as conferring powers to address the threat of ransomware would undermine the careful deliberations of Congress and the central reason for the statute's existence. Congress drafted IEEPA with the express purpose of conferring powers "more limited in scope" than those in TWEA. If ransomware attacks—a daily, ongoing issue for thousands of U.S. organizations—were interpreted as "unusual and extraordinary" or "rare and brief," the scope of powers under the IEEPA would match the vastness of those under TWEA. IEEPA, like its predecessor, would devolve into a "general grant of legislative authority to the President."[137] Because OFAC's policy conflicts with IEEPA's central purpose, it cannot fall within its scope.

2. OFAC's Policy Is Incompatible with Congress's Prescribed Mechanism for Combatting Ransomware Attacks

OFAC's policy is at the "lowest ebb" of authority as it conflicts with Congress's mechanism for combatting ransomware attacks. Because CIRCIA specifically addresses the issue of ransomware payments, OFAC is not free to take inconsistent measures based on Congress's failure to legislate.

As explained in Justice Jackson's *Youngstown* concurrence, executive action may be at its "lowest ebb" of authority when it is incompatible with the expressed or implied will of Congress.[138] In these circumstances, the executive is entitled only to "[its] own constitutional powers minus any constitutional powers of Congress over the matter."[139] If Congress passes legislation addressing an issue, the executive cannot take "different and inconsistent" measures and claim that the action was "necessitated or invited by failure of Congress to legislate upon the occasions."[140] For example, in *Youngstown*, Congress specifically prescribed a mechanism for settling labor disputes and rejected an amendment that would have

---

134 H. COMM. ON INT'L RELS., 95TH CONG., REVISION OF THE TRADING WITH THE ENEMY ACT: MARKUP BEFORE THE COMMITTEE ON INTERNATIONAL RELATIONS 5 (Comm. Print 1977).

135 H. COMM. ON INT'L RELS., 95TH CONG., TRADING WITH THE ENEMY ACT REFORM LEGISLATION, H.R. REP. No. 95-459, at 10 (1977) (Conf. Rep.).

136 *Id.* at 2.

137 *Id.* at 9.

138 Youngstown Sheet & Tube Co. v. Sawyer, 343 U.S. 579, 637 (1952) (Jackson, J., concurring).

139 *Id.*

140 *Id.* at 639.

allowed the president to seize property during emergencies.[141] Because the president's actions contradicted the method Congress prescribed and lacked authorization by the Constitution, the Court held his actions unconstitutional.[142]

OFAC's policy, like the president's seizure in *Youngstown*, contradicts the express will of Congress. In *Youngstown*, the president was not free to take any measures to resolve labor disputes—Congress specifically prescribed a mechanism for doing so in the Taft-Hartley Act.[143] In this case, Congress prescribed a mechanism for curbing ransomware attacks in CIRCIA: a mandatory reporting scheme paired with comprehensive liability protections.[144] Thus, OFAC cannot take inconsistent measures by imposing strict liability on victims and claim that the policy is "necessitated or invited by failure of Congress to legislate upon the occasion."[145]

While, unlike the situation in *Youngstown*, Congress did not specifically reject OFAC's policy, it nevertheless considered four different cyber incident reporting bills before passing CIRCIA.[146] It is, therefore, substantially unlikely that Congress failed to consider the possibility of imposing strict liability civil penalties for ransomware payments; it is more likely that Congress simply found it unwise to do so.

3. OFAC's Policy Is Not Implicitly Authorized By Congress: There Is No History of Congressional Acquiescence to the Executive's Authority to Issue Such a Policy

Congress did not implicitly authorize OFAC's policy as it is unsupported by congressional "inertia, indifference, or acquiescence." Congress's passage of CIRCIA signifies its refusal to acquiesce in the executive's authority to impose strict liability penalties on ransomware victims.

In Justice Jackson's second *Youngstown* category, executive action resides in a "zone of twilight" when Congress has neither authorized nor prohibited an action.[147] In these situations, congressional "inertia, indifference, or acquiescence" may invite executive action.[148] The Court applied this principle in *Dames & Moore* as it considered whether the

---

141 *Id.* at 585–89 (majority opinion).

142 *Id.* at 588–89.

143 *Id.* at 585–89.

144 Cyber Incident Reporting for Critical Infrastructure Act of 2022, Pub. L. No. 117-103, §§ 2242(a), 2245(b)–(e), 136 Stat. 1038, 1042–43, 1053–54 (codified at 6 U.S.C. §§ 681b, 681e).

145 *Youngstown*, 343 U.S. at 639 (Jackson, J., concurring).

146 PROPOSED INCIDENT REPORTING BILLS, *supra* note 35.

147 *Youngstown*, 343 U.S. at 637 (Jackson, J., concurring).

148 *Id.*

president had the authority to issue claim settlement agreements.[149] The Court looked to a long history of congressional acquiescence to the executive's authority to issue such agreements and held that the action was authorized as Congress implicitly approved of the practice.[150] Specifically, the Court found persuasive that Congress conferred broad discretionary power to the executive in the areas of emergencies and hostage negotiation and drafted legislation on the assumption that the president could issue such agreements.[151] As the Court explained, "A long-continued practice, known to and acquiesced in by Congress, . . . raise[s] a presumption that the [action] had been [taken] in pursuance of is consent."[152]

But Congress has not implicitly authorized the executive to impose strict liability penalties on ransomware victims. As an initial matter, there is no "long-continued practice" of executive agencies imposing such penalties on ransomware victims in which Congress could acquiesce. Moreover, since Congress passed CIRCIA within two years of OFAC first announcing its policy,[153] CIRCIA signifies Congress's refusal to acknowledge the executive's authority to issue such a policy. In *Dames*, congressional action implicitly recognized the executive's authority to issue claim settlement agreements.[154] Here, congressional action implicitly rejects the executive's authority to impose strict liability penalties for ransomware payments. Thus, even if IEEPA granted the executive with broad discretionary powers in the field of ransomware, CIRCIA represents the revocation of that authority.

OFAC cannot claim that congressional "inertia, indifference, or acquiescence" implicitly authorizes its policy. Far from expressing apathy over the ransomware issue, Congress researched the problem, considered potential solutions, and prescribed a mechanism for solving the issue. OFAC should follow Congress's lead.

4. OFAC's Policy Is Not Authorized by the Constitution Because, Following the Implementation of CIRCIA, It Will Only Tenuously Relate to National Security

Defenders of OFAC's policy might argue that combatting ransomware attacks is a matter of national security and therefore falls within the executive's Article II powers. This argument ignores the reality

---

149 Dames & Moore v. Regan, 453 U.S. 654, 679, 684 (1981).

150 *Id.* at 686–90.

151 *Id.* at 686.

152 *Id.* at 686 (second and third alteration in original) (quoting United States v. Midwest Oil Co., 263 U.S. 459, 474 (1915)).

153 Cyber Incident Reporting for Critical Infrastructure Act of 2022, Pub. L. No. 117-103, 136 Stat. 1038 (codified at 6 U.S.C. §§ 681–681g); OFAC ADVISORY, *supra* note 1.

154 *Dames*, 453 U.S. at 686.

of OFAC's policy and the entities subject to enforcement. CIRCIA provides "covered entities" with liability protections from government enforcement actions.[155] "Covered entities" are organizations within sixteen critical infrastructure sectors "vital to . . . the Nation's safety, prosperity, and wellbeing."[156] Under CIRCIA's mandatory reporting scheme, these organizations will be effectively immune from OFAC's policy so long as they comply with the statute's reporting requirements. By default, then, OFAC's policy will apply almost exclusively to organizations in non-critical infrastructure sectors, or organizations not "vital to the Nation's safety." The executive's national security authority cannot authorize OFAC's policy when it will apply only to organizations deemed insignificant to national security.

As Justice Black explained in *Youngstown*, the executive's power, if any, to take an action "must stem either from an act of Congress or from the Constitution itself."[157] OFAC's policy stems from neither. The policy is not authorized by IEEPA as it conflicts with the statute's text, legislative intent, and central purpose. The policy is at the "lowest ebb" of authority as it contradicts Congress's mechanism for curbing ransomware payments, as expressed in CIRCIA. The policy is not implicitly authorized by Congress as there is no history of congressional acquiescence to the executive's authority to issue such a policy. Lastly, the policy is not authorized by the Constitution as it only tenuously relates to national security interests.

B. *The Policy Concerns: OFAC's Policy Incentivizes Victims to Cover Up Their Attacks*

In addition to the legal issues discussed above, OFAC's policy has a fundamental flaw: it disincentivizes victims from sharing information on ransomware attacks with the government. OFAC's policy discourages information sharing in two steps. First, as discussed in Subsection 1, OFAC's policy does not meaningfully deter ransom payments as the cost of not paying a ransom often outweighs the risk of OFAC penalties. Second, as discussed in Subsection 2, once a victim has made a ransom payment, OFAC's policy discourages information sharing through its strict liability threat. With this incentive structure, OFAC's policy serves only to worsen the lack of information sharing between ransomware victims and the government.

---

155 Cyber Incident Reporting for Critical Infrastructure Act of 2022 § 2240(5).

156 Presidential Policy Directive, *supra* note 41.

157 Youngstown Sheet & Tube Co. v. Sawyer, 343 U.S. 579, 585 (1952).

1. OFAC's Policy Does Not Have a Significant Deterrent Effect on Ransom Payments

While OFAC's policy threatens to punish ransomware victims for ransom payments, it does not significantly deter them from doing so. Because the cost of refusing to pay a ransom is often exponentially higher than the ransom itself, and the likelihood of OFAC penalties is significantly low, many organizations may rationally choose to pay the ransom.

First, OFAC's policy underestimates the cost of refusing to pay attackers' ransom demands. While ransomware demands have increased over recent years,[158] the cost of operational downtime may exceed fifty times the ransom itself.[159] In many situations, refusal to pay may result in substantial, real-life harm to both the victim organization and its clients, patients, or shareholders. For example, for the lawyer in the opening hypothetical, refusal to pay the ransom could result in the disclosure of clients' confidential information or missed filing deadlines. While there is no guarantee that a ransom payment will result in decryption, in these situations and many others, paying a ransom may be the best option to avoid harm to the victim organization and downstream parties.

Second, a victim could reasonably infer that the likelihood of an OFAC penalty for a ransom payment is extremely low. For OFAC to penalize a ransomware victim for a payment, (1) the attacker must be on the SDN List, and (2) OFAC must discover the payment.[160] However, it is unlikely that a victim's attacker would be on OFAC's SDN List as cybercriminals routinely re-brand to evade sanctions.[161] Further, it is unlikely that OFAC would discover the payment given the lack of government access to ransomware information.[162] As the government is combatting ransomware in the dark, a victim's payment is unlikely to come to light. Lastly, if there were any remaining doubts as to the likelihood of an OFAC penalty, the victim could simply look to OFAC's track record under this policy: OFAC has yet to fine an organization for a ransom payment to an attacker on its SDN List.[163] From these observations, a victim could easily and reasonably deduce that OFAC's policy is an empty threat.

---

158 NSI *Report*, *supra* note 19; COVEWARE *Report*, *supra* note 17.

159 DATTO *Report*, *supra* note 20.

160 OFAC ADVISORY, *supra* note 1, at 3–4.

161 *See*, *e.g.*, Muncaster, *supra* note 56.

162 SENATE REPORT, *supra* note 4, at 5.

163 Timothy O'Toole, Christopher Stagg, FeiFei Ren, Caroline Watson, Manuel Levitt & Samuel Cutler, *Practical Issues in Cyber-Related Sanctions*, GLOB. INVESTIGATIONS REV. (Sept. 29, 2023), https://perma.cc/T4ER-XEVM.

2. OFAC's Threat of Strict Liability Discourages Any Victim Who Paid a Ransom from Sharing Information with the Government

By threatening victims with strict liability, OFAC's policy discourages victims who paid a ransom from sharing information with the government. Because victims are at the mercy of OFAC's discretion to reduce penalties, victims are incentivized to cover up their ransom payments.

Unlike the reporting framework in CIRCIA, OFAC's policy starts with a presumption of liability for payments made to attackers on its SDN List.[164] Once OFAC discovers of a payment, liability can be reduced only if the victim presents mitigating factors that OFAC finds sufficient.[165] OFAC has suggested that a penalty may be reduced if a victim organization has adequate cybersecurity hygiene and complies with law enforcement.[166] Ultimately, however, the amount of a given fine is up to the discretion of OFAC's director.[167]

Because OFAC's policy is based on strict liability, any ransomware victim who pays a ransom may rationally decide to cover up an attack. Given that ransomware attacks are typically anonymous, it would be difficult, if not impossible, to discover whether an attacker is on OFAC's SDN List.[168] Thus, unless victims can confirm the identity of their attacker, there remains a possibility that their payment violated OFAC's policy.

A victim who paid a ransom has two options: report the information to the government or cover up the attack. If a victim discloses the payment to the government and the attacker happens to be on OFAC's list, the victim would be presumed liable. While OFAC would likely consider voluntary disclosure as a mitigating factor, the victim would ultimately fall to the mercy of OFAC's discretion in determining the penalty.[169] OFAC could, for instance, determine that the victim did not practice adequate cyber hygiene and is therefore deserving of punishment. On the other hand, for the reasons highlighted above, it may be substantially unlikely that OFAC would discover the payment if a victim covered up the attack. Without concrete liability protections and only discretionary mitigating factors, covering up may be the best option.

Defenders of OFAC's policy may claim that, although it may not incentivize information sharing, the primary purpose of the policy is to reduce the profitability of ransomware attacks for cybercriminals. While this may be a legitimate goal, it underestimates the importance of information for ransomware law enforcement. As the government knows

---

164 OFAC ADVISORY, *supra* note 1, at 3–4.

165 *Id.* at 5.

166 *Id.*

167 *Id.*

168 Westbrook, *supra* note 3, at 415–17.

169 OFAC ADVISORY, *supra* note 1, at 5.

of only approximately 25% of ransomware attacks, law enforcement is handcuffed in combatting the ransomware threat.[170] The urgent need for ransomware information is evident in CIRCIA's framework: by mandating reporting and providing victims with liability protection, Congress signaled that information is the top priority in ransomware regulation.

Conclusion

OFAC's threat of strict liability civil penalties for ransomware payments is both unlawful and a bad idea. From a legal perspective, the policy lacks authority from either an act of Congress or the Constitution. From a policy perspective, it discourages victims from sharing ransomware information with the government. The rise in ransomware attacks is not a simple problem to solve, and this Comment does not attempt to do so. As with solving any difficult problem, however, information is key. By passing CIRCIA, Congress recognizes as much. If OFAC renounces its policy and defers to the judgment of Congress, it may take one step towards bringing the ransomware issue to light.

170 SENATE REPORT, *supra* note 4, at 5.