Boston College Law Review

Volume 63
Issue 9 *Electronic Supplement*

Article 14

5-9-2022

Ransomware, Cyber Sanctions, and the Problem of Timing

Christine Abely
New England Law | Boston, cabely@nesl.edu

RANSOMWARE, CYBER SANCTIONS, AND THE PROBLEM OF TIMING

CHRISTINE ABELY*

Abstract: This essay argues that the lack of a federal blanket prohibition against ransomware payments undermines the purpose and effectiveness of the U.S. sanctions regime. The U.S. cyber-related sanctions program suffers from an essential problem of timing: often payments to malicious cyber actors are not prohibited until those actors have been named to the Specially Designated Nationals and Blocked Persons List (SDN) maintained by the Office of Foreign Assets Control in the U.S. Department of the Treasury. Yet those actors generally are not so designated until they have been identified as malicious through a completed or attempted attack. Further, the time between a cyberattack and the designation of a party as an SDN is generally not short enough to prohibit the making of a ransomware payment in response to an attack itself. A blanket prohibition against the making of ransomware payments would supplement the OFAC regulations and remedy a structural shortcoming of that regulatory scheme.

INTRODUCTION

Ransomware attacks against U.S.-based targets, and across the world, have been rising in recent years.[1] These attacks block access to a victim's systems or data until the target "pay[s] a ransom to the attacker[]."[2] Ransomware attacks have struck a broad variety of organizations including "educational institutions . . . hospitals, pipelines, private companies, grocery stores and local

* Faculty Fellow, New England Law | Boston. J.D., University of Virginia School of Law; B.A., Dartmouth College.

[1] Lynsey Jeffery & Vignesh Ramachandran, *Why Ransomware Attacks Are on the Rise—and What Can Be Done to Stop Them*, PBS NEWSHOUR (July 8, 2021, 3:28 PM), https://www.pbs.org/newshour/nation/why-ransomware-attacks-are-on-the-rise-and-what-can-be-done-to-stop-them [https://perma.cc/Q7SN-HUW2] (conveying that cybersecurity firm SonicWall determined that "ransomware attacks rose by 62 percent worldwide, and by 158 percent in North America"); Brenda R. Sharton, *Ransomware Attacks Are Spiking. Is Your Company Prepared?*, HARVARD BUS. REV. (May 20, 2021), https://hbr.org/2021/05/ransomware-attacks-are-spiking-is-your-company-prepared [https://perma.cc/LC3K-5B9P]. *But see* Alex Scroxton, *Ransomware Attacks Dropped 37% in December, Claims NCC*, COMPUTERWEEKLY.COM (Jan. 20, 2022), https://www.computerweekly.com/news/252512245/Ransomware-attacks-dropped-37-in-December-claims-NCC [https://perma.cc/ZMF8-DV4E] (explaining that the reported decrease in ransomware attacks could be explained by seasonal factors).

[2] Jeffery & Ramachandran, *supra* note 1.

governments."[3] In 2021, attackers deployed ransomware against water treatment plants in California, Maine, and Nevada.[4] The ransomware attack against the Colonial Pipeline that same year temporarily shut down the supply line for "nearly half the . . . fuel used on the U.S. East Coast."[5] The stakes associated with these attacks are high, as affected operations may be vitally important to industry or to the country as a whole.

Ransomware originating from Russian actors in particular remains a threat to U.S. entities and beyond. Ransomware attacks are often linked to Russian-based actors; indeed, "roughly 74% of ransomware revenue in 2021 – over $400 million worth of cryptocurrency – went to strains . . . highly likely to be affiliated with Russia in some way."[6] Ransomware attacks to the U.S. and other countries that take measures against Russia for its invasion of Ukraine are a present threat, although such cyberattacks might be made for disruptive and retaliatory purposes rather than the seeking of a ransom.[7]

---

[3] Madeleine Ngo, *Howard University Hit by a Ransomware Attack*, N.Y. TIMES (Sept. 7, 2021), https://www.nytimes.com/2021/09/07/education/howard-university-ransomware.html [https://perma.cc/3D45-77WC]; *see* Stacy Weiner, *The Growing Threat of Ransomware Attacks on Hospitals*, ASS'N OF AM. MED. COLLS. (July 20, 2021), https://www.aamc.org/news-insights/growing-threat-ransomware-attacks-hospitals [https://perma.cc/BPN6-UZP4] (describing the threats posed by ransomware to medical facilities). *See generally* Tom C.W. Lin, *Business Warfare*, 63 B.C. L. REV. 1 (2022) (examining "contemporary business warfare," which involves attacks perpetrated by both "state and nonstate adversaries" and providing additional examples of recent cyberattacks).

[4] *Alert (AA21-287A): Ongoing Cyber Threats to U.S. Water and Wastewater Systems*, CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY, https://www.cisa.gov/uscert/ncas/alerts/aa21-287a [https://perma.cc/5LZZ-9B5Z] (Oct. 25, 2021).

[5] Gloria Gonzalez, Ben Lefebvre & Eric Geller, *'Jugular' of the U.S. Fuel Pipeline System Shuts Down After Cyberattack*, POLITICO (May 8, 2021), https://www.politico.com/news/2021/05/08/colonial-pipeline-cyber-attack-485984 [https://perma.cc/3GTC-ZR9Y].

[6] Chainalysis Team, *Russian Cybercriminals Drive Significant Ransomware and Cryptocurrency-based Money Laundering Activity*, CHAINALYSIS (Feb. 14, 2022), https://blog.chainalysis.com/reports/2022-crypto-crime-report-preview-russia-ransomware-money-laundering/ [https://perma.cc/MS6X-5AWE]; *see* Sean Lyngaas, *US Security and Intelligence Agencies Prep for Potential Russian Hacking Threats*, CNN POLITICS, https://www.cnn.com/2022/02/12/politics/us-security-intelligence-prep-russian-hacking-threats/index.html [https://perma.cc/3QE4-RQ3M] (Feb. 14, 2022) ("Officials from the FBI and the Department of Homeland Security briefed state and local government officials . . . on potential Russian hacking threats . . . .").

[7] *See, e.g.*, Eric Geller, *Russian Ransomware Gang Threatens Countries That Punish Moscow for Ukraine Invasion*, POLITICO (Feb. 25, 2022), https://www.politico.com/news/2022/02/25/russian-ransomware-gang-threatens-countries-ukraine-00011896 [https://perma.cc/YXR7-76UC] (providing information about the current threat environment); Jena M. Valdetero, *Preparing for the Possibility of Russian Ransomware Attacks*, NAT'L L. REV. (Feb. 26, 2022), https://www.natlawreview.com/article/preparing-possibility-russian-ransomware-attacks [https://perma.cc/7WHC-GRSP] (providing suggestions for companies to ensure they are prepared to deal with such threats); *Shields Up*, CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY, https://www.cisa.gov/shields-up [https://perma.cc/67GQ-FQAH] (providing guidance for organizations about the current cyber threats posed by Russia's invasion of Ukraine).

The Office of Foreign Assets Control (OFAC) in the U.S. Department of the Treasury issued advisories in October 2020 and September 2021 reminding those subject to the U.S. sanctions laws that ransomware payments are subject to the same sanctions restrictions as are other types of payments.[8] Ransomware payments may violate U.S. sanctions provisions in several ways, such as if they are made to a person or entity listed on the Specially Designated Nationals and Blocked Persons (SDN) List, whether through the Cyber-Related Sanctions program or otherwise. Ransomware payments may also violate the sanctions regulations if they are made to a person or entity located in a comprehensively-embargoed country or region and no relevant exception or license applies, or if they involve the use of U.S. dollars or are facilitated by a U.S. party.[9] Thus many ransomware payments are prohibited by the U.S. sanctions regulations. But not all are—for example, if they involve a previously unknown attacker not yet designated as an SDN, and where no other sanctions restrictions are implicated.

To address the growing threat of ransomware attacks, lawmakers have considered banning ransomware payments entirely. States including New York, North Carolina, Pennsylvania, Florida, and Texas have considered enacting such outright bans.[10] There has also been some discussion of a ban at the federal level.[11]

This essay argues that the lack of a federal blanket prohibition against ransomware payments undermines the purpose and effectiveness of the U.S. sanctions regime. The U.S. cyber-related sanctions program suffers from an

---

[8] U.S. DEP'T OF THE TREASURY, ADVISORY ON POTENTIAL SANCTIONS RISKS FOR FACILITATING RANSOMWARE PAYMENTS (2020) [hereinafter 2020 RANSOMWARE PAYMENTS ADVISORY], https://home.treasury.gov/system/files/126/ofac_ransomware_advisory_10012020_1.pdf [https://perma.cc/N9D5-4FGC]; U.S. DEP'T OF THE TREASURY, UPDATED ADVISORY ON POTENTIAL SANCTIONS RISKS FOR FACILITATING RANSOMWARE PAYMENTS (2021) [hereinafter 2021 UPDATED RANSOMWARE PAYMENTS ADVISORY], https://home.treasury.gov/system/files/126/ofac_ransomware_advisory.pdf [https://perma.cc/H75K-3ZSA].

[9] *See infra* Section I.A.

[10] Jenni Bergal, *States Weigh Bans on Ransomware Payoffs*, PEW CHARITABLE TRS. (July 23, 2021), https://www.pewtrusts.org/en/research-and-analysis/blogs/stateline/2021/07/23/states-weigh-bans-on-ransomware-payoffs [https://perma.cc/AGR3-EBFU] (summarizing recent developments in state legislatures); Lawrence Mower, *Florida Lawmakers Want a 'No Negotiation' Policy with Ransomware Attackers*, TAMPA BAY TIMES (Feb 3, 2022), https://www.tampabay.com/news/florida-politics/2022/02/03/florida-lawmakers-want-a-no-negotiation-policy-with-ransomware-attackers/ [https://perma.cc/58F2-4KPR].

[11] Chris Matthews, *Congress May Ban Ransomware Payments, Senate Homeland Security Chairman Says*, MARKETWATCH (Oct. 26, 2021), https://www.marketwatch.com/story/congress-may-ban-ransomware-payments-senate-homeland-security-chairman-says-11635264388 [https://perma.cc/RWS3-DEHU] ("Lawmakers have not ruled out legislation that could ban private companies from making ransomware payments . . . ." (citing Senator Gary Peters of Michigan, Chairman, Senate Homeland Security Committee)).

essential problem of timing: often payments to malicious cyber actors are not prohibited until those actors have been named to the SDN List. Yet those actors generally are not so designated until they have been identified as malicious through a completed or attempted attack. Further, the time between a cyberattack and the designation of a party as an SDN is generally not short enough to prohibit the making of a ransomware payment in response to an attack itself. A blanket prohibition against the making of ransomware payments would supplement the OFAC regulations and remedy a structural shortcoming of that regulatory scheme.

I. LEGAL STRUCTURE

A. Sanctions Restrictions

Sanctions are administered by the Office of Foreign Assets Control (OFAC) within the U.S. Department of the Treasury.[12] Financial transactions involving persons or entities contained on the Specially Designated Nationals (SDN) List are proscribed.[13] Other sanctions regulations restrict payments made to countries or geographic areas,[14] although some purposes are excepted or licensed from the scope of those prohibitions.[15] U.S. persons are also prohibited from facilitating payments to parties conducting activities that would be illegal if conducted by a U.S person or entity.[16] U.S. persons are also pro-

---

[12] *Office of Foreign Assets Control—Sanctions Programs and Information*, U.S. DEP'T OF THE TREASURY, https://home.treasury.gov/policy-issues/office-of-foreign-assets-control-sanctions-programs-and-information [https://perma.cc/U5E5-8WBX].

[13] *Specially Designated Nationals and Blocked Persons List (SDN) Human Readable Lists*, U.S. DEP'T OF THE TREASURY, https://home.treasury.gov/policy-issues/financial-sanctions/specially-designated-nationals-and-blocked-persons-list-sdn-human-readable-lists [https://perma.cc/W9H2-2BLX] (Mar. 18, 2022) ("[SDNs'] assets are blocked and U.S. persons are generally prohibited from dealing with them.").

[14] Court E. Golumbic & Robert S. Ruff III, *Leveraging the Three Core Competencies: How OFAC Licensing Optimizes Holistic Sanctions*, 38 N.C. J. INT'L L. & COM. REGUL. 729, 733–34 (2013).

[15] *See, e.g.*, OFF. OF FOREIGN ASSETS CONTROL, U.S. DEP'T OF THE TREASURY, FACT SHEET: PROVISION OF HUMANITARIAN ASSISTANCE AND TRADE TO COMBAT COVID-19 (2020), https://home.treasury.gov/system/files/126/covid19_factsheet_20200416.pdf [https://perma.cc/3GUK-DDMF] (detailing "the most relevant exemptions, exceptions, and authorizations for humanitarian assistance and trade under the OFAC-administered Iran, Venezuela, North Korea, Syria, Cuba, and Ukraine/Russia-related sanctions programs").

[16] *Financial Sanctions Frequently Asked Questions, Question 497: In Providing Services Consistent with the Compliance Services Guidance to a Foreign Covered Person, Can a U.S. Person Opine on the Legality of a Transaction Under U.S. Sanctions Laws, Including by Providing a Legal Opinion, Certification, or Other Clearance as to the Legality of Such Transaction, Where It Would Be Prohibited for a U.S. Person to Engage in Such Transaction?*, OFF. OF FOREIGN ASSETS CONTROL, U.S. DEP'T OF THE TREASURY (Jan. 12, 2017), https://home.treasury.gov/policy-issues/financial-sanctions/faqs/497 [https://perma.cc/7Y99-JANY] ("U.S. persons, wherever located, may not otherwise approve, finance, facilitate, or guarantee any transaction by a foreign person . . . where the trans-

hibited from causing a violation of the sanctions laws.[17] Causing a violation of the sanctions laws can, for example, occur through transacting in U.S. dollars abroad and engaging a U.S. financial institution in the dollar-clearing process.[18]

On April 1, 2015, President Obama issued E.O. 13694.[19] This order authorized the blocking of certain persons engaging in significant malicious cyber-related activities.[20] The order was issued based on "the increasing prevalence and severity of malicious cyber-enabled activities originating from, or directed by persons located . . . outside the United States [which] constitute an unusual and extraordinary threat to the national security, foreign policy, and economy of the United States."[21] Subsequently, OFAC issued the Cyber-Related Sanctions Regulations to put these restrictions into effect.[22] President Obama thereafter issued Executive Order 13757, which further sanctioned parties determined "to be responsible for or complicit in, or to have engaged in, directly or indirectly, cyber-enabled activities originating from, or directed by persons . . . outside the United States" related to "significant threat[s] to the national security, foreign policy, or economic health or financial stability of the United States" among other requirements.[23]

On April 15, 2021, President Biden issued E.O. 14024, which authorized the blocking of persons named by the Secretary of the Treasury as having engaged, or attempted to engage, in activities on behalf or for the benefit of the Russian government including "malicious cyber-enabled activities."[24]

---

action by that foreign person would be prohibited . . . if performed by a U.S. person or within the United States.").

[17] *See, e.g.*, *Financial Sanctions Frequently Asked Questions, Question 1,021: Do the Prohibitions of Executive Order (E.O.) 14024 and Other Russia-related Sanctions Extend to Virtual Currency?*, OFF. OF FOREIGN ASSETS CONTROL, U.S. DEP'T OF THE TREASURY (Mar. 11, 2022), https://home.treasury.gov/policy-issues/financial-sanctions/faqs/1021 [https://perma.cc/M3TE-Q9DM]; Christine Abely, *Causing a Sanctions Violation with U.S. Dollars: Differences in Regulatory Language Across OFAC Sanctions Programs*, 48 GA. J. INT'L & COMP. L. 29, 44 (2019).

[18] Abely, *supra* note 17, at 44.

[19] Exec. Order No. 13,694, 80 Fed. Reg. 18,077 (Apr. 1, 2015), *order amended by* Exec. Order No. 13,757, 82 Fed. Reg. 1 (Dec. 28, 2016).

[20] *Id.* § 1(a) ("All property and interests in property that are in the United States, that hereafter come within the United States, or that are or hereafter come within the possession or control of any United States person of the following persons are blocked and may not be transferred, paid, exported, withdrawn, or otherwise dealt in . . . .").

[21] *Id.* at intro.

[22] Cyber-Related Sanctions Regulations, 31 C.F.R. pt. 578 (2021).

[23] Exec. Order No. 13,757, 82 Fed. Reg. 1 (Dec 28, 2016).

[24] Exec. Order No. 14,024, 86 Fed. Reg. 20,249 (Apr. 15, 2021), *supplemented by* Exec. Order No. 14,066, 87 Fed. Reg. 13,625 (Mar. 8, 2022).

B. Other Legal Provisions

Other legal tools besides sanctions exist to combat ransomware attacks. These include federal criminal laws "such as the Computer Fraud and Abuse Act"; "statutes criminalizing conspiracy and aiding and abetting"; "federal cybersecurity laws"; and "data protection laws."[25]

The White House convened a virtual summit in October 2021 to discuss the ransomware threat, with delegates from more than thirty nations in attendance.[26] Those representatives subsequently issued a statement calling for actions to build "network resilience," frustrate ransomware activities through law enforcement, "[c]ounter [i]llicit [f]inance," and engage in diplomacy.[27]

Legislation was introduced to Congress in fall 2021 that would require "disclos[ure] of information about ransom[ware] payments" within 48 hours of being made.[28] Similarly, in November 2021, legislation was introduced to require reporting to the U.S. Department of the Treasury of ransomware payments as well as approval from law enforcement to make such payments "in excess of $100,000."[29] Language that would have mandated ransomware reporting was ultimately cut from the National Defense Authorization Act.[30]

II. OFAC Advisories and Sanctions Risks

A. Advisories

OFAC discussed many of the sanctions risks around ransomware payments in an October 1, 2020 advisory.[31] It advised entities, including both those making ransomware payments and those assisting ransomware victims in

---

[25] Peter G. Berris & Jonathan M. Gaffney, Cong. Rsch. Serv., R46932, Ransomware and Federal Law: Cybercrime and Cybersecurity, at summary (2021).

[26] Jenna McLaughlin, *White House Brings Together 30 Nations to Combat Ransomware*, NPR (Oct. 13, 2021), https://www.npr.org/2021/10/13/1045248842/white-house-brings-together-30-nations-to-combat-ransomware [https://perma.cc/XT56-TRZH].

[27] Press Release, White House, Joint Statement of the Ministers and Representatives from the Counter Ransomware Initiative Meeting October 2021 (Oct. 14, 2021), https://www.whitehouse.gov/briefing-room/statements-releases/2021/10/14/joint-statement-of-the-ministers-and-representatives-from-the-counter-ransomware-initiative-meeting-october-2021/ [https://perma.cc/SMN5-U6XJ].

[28] *Warren & Ross Introduce Bill to Require Disclosures of Ransomware Payments*, Elizabeth Warren (Oct. 5, 2021), https://www.warren.senate.gov/newsroom/press-releases/warren-and-ross-introduce-bill-to-require-disclosures-of-ransomware-payments [https://perma.cc/527T-FZYX].

[29] Press Release, U.S. Congressman Patrick McHenry, McHenry Introduces Bill to Protect America's Critical Financial Infrastructure from Ransomware Attacks (Nov. 10, 2021), https://mchenry.house.gov/news/documentsingle.aspx?DocumentID=403073 [https://perma.cc/9UK9-VKCW].

[30] Joseph Marks, *Congress Can't Even Pass the Easy Cyber Stuff*, Wash. Post (Dec. 8, 2021), https://www.washingtonpost.com/politics/2021/12/08/congress-cant-even-pass-easy-cyber-stuff/ [https://perma.cc/T7RP-P5PS].

[31] 2020 Ransomware Payments Advisory, *supra* note 8.

doing so "to implement a risk-based compliance program."[32] OFAC noted the particular importance of ensuring that an "SDN or blocked person, or a comprehensively embargoed jurisdiction" was not involved in the transaction.[33] The advisory specifically referenced the applicability of its guidance to "financial institutions" as well as "companies that engage with victims of ransomware attacks, such as those involved in providing cyber insurance, digital forensics and incident response, and financial services that may involve processing ransom payments (including depository institutions and money services businesses)."[34]

In September 2021, OFAC issued an updated, superseding advisory which listed steps that companies could take that would "be considered . . . significant mitigating factor[s] in any [potential] enforcement [action].[35] These included "a company's full and ongoing cooperation with law enforcement . . . [which may involve] providing all relevant information such as technical details, ransom payment demand, and ransom payment instructions as soon as possible," as well as "adopting or improving cybersecurity practices."[36] The advisory "strongly discourage[d] the payment of cyber ransom or extortion demands" and warned of the ways in which such payments might violate OFAC regulations.[37]

Also in September 2021, the U.S. Treasury announced a variety of actions to respond to ransomware threats, including adding the "virtual currency exchange" SUEX to its SDN List.[38] The Financial Crimes Enforcement Network (FinCEN) worked "to collect information relating to ransomware payments."[39] According to the Treasury press release, "over 40% of SUEX's known transaction history is associated with illicit actors," and the exchange had "facilitated transactions involving illicit proceeds from at least eight ransomware variants."[40]

---

[32] *Id.* at 3.

[33] *Id.* at 4.

[34] *Id.* at 3–4.

[35] 2021 UPDATED RANSOMWARE PAYMENTS ADVISORY, *supra* note 8, at 4–5.

[36] *Id.* (citing MULTI-STATE INFO. SHARING & ANALYSIS CTR., CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY, RANSOMWARE GUIDE SEPTEMBER 2020, https://www.cisa.gov/sites/default/files/publications/CISA_MS-ISAC_Ransomware%20Guide_S508C_.pdf [https://perma.cc/ZVC2-9RSK]).

[37] *Id.* at 1, 3.

[38] Press Release, U.S. Dep't of the Treasury, Treasury Takes Robust Actions to Counter Ransom ware (Sept. 21, 2021), https://home.treasury.gov/news/press-releases/jy0364 [https://perma.cc/QZ7X-3CRW].

[39] *Id.*

[40] *Id.*

B. Sanctions Risks

Even in the absence of a blanket ban on ransomware payments, those companies who choose to make ransomware payments face heightened risks of violating the U.S. sanctions laws. Of course, an organization must screen a cyber attacker to whom it is making a payment to ensure that it is not contained on the SDN List.[41] Geographic considerations also exist: the payment must not be made to a person or entity located within a "comprehensively embargoed" region or country.[42]

The currency used in a particular transaction may create a connection for U.S. jurisdiction. The use of U.S. dollars, even when transacted between two non-U.S. parties, carries a high likelihood of a sanctions violation due to the nature of the dollar-clearing system, in which U.S. financial institutions often play a role.[43] As OFAC guidance makes clear, payments when made in cryptocurrency must also adhere to the requirements of the U.S. sanctions regulations.[44] Indeed, the listing of SUEX on the SDN List was made in response to the exchange's role in abetting illegal ransomware payments through cryptocurrency.[45]

III. THE PROBLEM OF TIMING

The OFAC sanctions regulations successfully prohibit transactions to many malicious cyber actors, but notable gaps remain in the regulatory scheme. Given the purpose of the sanctions program targeting malicious cyber actors, allowing ransomware payments to be made to those cyber attackers not yet contained on the SDN List undercuts the purposes of the U.S. sanctions regime.

Cyber attackers are often necessarily listed only *after* they have used or attempted to use technology to hold companies' resources or operations hos-

---

[41] 2021 UPDATED RANSOMWARE PAYMENTS ADVISORY, *supra* note 8, at 4.

[42] *Id.*

[43] *See, e.g.,* Brad Karp et al., *OFAC Breaks New Ground by Penalizing Non-U.S. Companies for Making U.S. Dollar Payments Involving a Sanctioned Country*, HARV. L. SCH. F. ON CORP. GOVERNANCE (Aug. 16, 2017), https://corpgov.law.harvard.edu/2017/08/16/ofac-breaks-new-ground-by-penalizing-non-u-s-companies-for-making-u-s-dollar-payments-involving-a-sanctioned-country/ [https://perma.cc/VY9D-V72K] (explaining how the OFAC has penalized foreign companies); *see also* Abely, *supra* note 17, at 44.

[44] *Financial Sanctions Frequently Asked Questions, Question 560: Are My OFAC Compliance Obligations the Same, Regardless of Whether a Transaction Is Denominated in Digital Currency or Traditional Fiat Currency?*, OFF. OF FOREIGN ASSETS CONTROL, U.S. DEP'T OF THE TREASURY (Mar. 19, 2018), https://home.treasury.gov/policy-issues/financial-sanctions/faqs/560 [https://perma.cc/RAL4-XHD6].

[45] Alexandra Alper, *Biden Sanctions Cryptocurrency Exchange Over Ransomware Attacks*, REUTERS (Sept. 21, 2021), https://www.reuters.com/business/finance/biden-sanctions-cryptocurrency-exchange-over-ransomware-attacks-2021-09-21/ [https://perma.cc/JEL8-5PFE].

tage.[46] The issue is primarily one of timing; the structure of the cyber-related sanctions program can be a reactive one. The process of identification and subsequently designating a party as an SDN is generally too slow to prohibit a ransomware payment after a ransomware attack has been made but before a ransom payment has been issued.[47] Indeed, where critically important functions are held hostage until a ransom is paid, there is immense pressure to pay a ransom as quickly as possible. For example, when cybercriminals attacked the Colonial Pipeline Co. in 2021, the company made a $5 million ransom payment within one day.[48]

Thus, after a ransomware attack has occurred, the OFAC sanctions programs were not designed, and do not actually function, to prohibit payments to those attackers immediately after the initial attack if existing sanctions regulations do not block the payment and if attackers are not yet designated as SDNs. Commentary has noted that the sanctions regulations are "not suited for [addressing] ransomware attacks," since those regulations "still need to be tied to a specific individual, entity or country to accomplish some larger goal."[49] A comprehensive prohibition on the making of any ransomware payments, whether or not the recipient is currently contained on the SDN List or is otherwise restricted by the sanctions provisions from receiving payments, would eliminate this issue of timing and more completely fulfill the purposes of the malicious cyber actors sanctions program and the U.S. sanctions regime as a whole. The sanctions regulations are imperfect tools for addressing the threat of ransomware payments by themselves, and the lack of a ban in some other form undermines the ability of the regulatory sanctions framework to address the ransomware threat coherently.

The purposes of other cyber-specific sanctions programs also align with a blanket ban on ransomware. In particular, the Russia-specific sanctions that were announced in April 2021 can also suffer from the same timing problem as

---

[46] *See*, *e.g.*, Press Release, U.S. Dep't of the Treasury, Treasury Sanctions Two Individuals for Malicious Cyber-Enabled Activities (Dec. 29, 2016), https://home.treasury.gov/news/press-releases/jl0693 [https://perma.cc/EQL9-N4JR] (providing examples of sanctions levied against individuals).

[47] *See, e.g.*, Press Release, U.S. Dep't of the Treasury, Treasury Continues to Counter Ransomware as Part of Whole-of-Government Effort; Sanctions Ransomware Operators and Virtual Currency Exchange (Nov. 8, 2021), https://home.treasury.gov/news/press-releases/jy0471 [https://perma.cc/8CZD-CP7B] (designating individuals in part for their participation in July 2021 ransomware activity); Press Release, U.S. Dep't of the Treasury, Treasury Sanctions North Korean State-Sponsored Malicious Cyber Groups (Sept. 13, 2019), https://home.treasury.gov/news/press-releases/sm774 [https://perma.cc/VU6X-D83E] (designating entities in conjunction with 2017 WannaCry attacks).

[48] Christina Wilkie, *Colonial Pipeline Paid $5 Million Ransom One Day After Cyberattack, CEO Tells Senate*, CNBC, https://www.cnbc.com/2021/06/08/colonial-pipeline-ceo-testifies-on-first-hours-of-ransomware-attack.html [https://perma.cc/L367-MJRU] (June 9, 2021).

[49] Alvaro Marañon & Benjamin Wittes, *Ransomware Payments and the Law*, LAWFARE (Aug. 11, 2021), https://www.lawfareblog.com/ransomware-payments-and-law [https://perma.cc/U58J-LHZN].

do the malicious cyber attacker regulations. Namely, even though malicious cyber attackers from Russia are blocked as soon as they are designated by the Secretary of the Treasury to be placed on the SDN List, payments to those actors are not barred before that time so long as they do not violate any other sanctions provision.[50] A blanket ban on ransomware payments would help to address this similar gap in the regulatory framework.

Nor do the other OFAC sanctions programs solve this problem of timing by themselves. OFAC's geographically-based restrictions are certainly expansive. But they do not by themselves address the specific problem of cyber attackers. Some cyber attackers are located outside of the geographic areas subject to OFAC bans, and therefore are only addressed by being placed on the SDN List.[51] The geographic bans are also naturally over-expansive with respect to specifically addressing the ransomware problem, in that they are often intended to address other issues.[52] A blanket ban on ransomware would specifically address the threat of cyber attackers without the over-expansiveness problem that would arise were OFAC to address the issue solely through the expansion of geographically-based sanctions.

A ban on ransomware payments would align with the purposes of the existing U.S. sanctions regulations concerning malicious cyber attackers.[53] There are certainly compelling reasons, however, as to why continuing to allow U.S. entities to make ransomware payments might be desirable for other reasons. Companies might resume vital operations if they were given the flexibility to

---

[50] *See. e.g.,* Exec. Order No. 13,757, 82 Fed. Reg. 1 (Dec. 28, 2016) (providing for blocking sanctions for "any person determined by the Secretary of the Treasury, in consultation with the Attorney General and the Secretary of State, *to be responsible for or complicit in, or to have engaged in* . . . cyber-enabled activities . . . that are reasonably likely to result in, or have materially contributed to, a significant threat to the national security, foreign policy, or economic health or financial stability of the United States" (emphasis added)).

[51] *See* MICROSOFT, MICROSOFT DIGITAL DEFENSE REPORT: OCTOBER 2021, at 55, https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWMFIi [https://perma.cc/8W4G-GU4A] (illustrating cyberattacks by source country, with 58% of attacks originating from Russia, 23% originating from North Korea, 11% originating from Iran, 8% originating from China, and less than 1% originating from South Korea, Vietnam, and Turkey, respectively).

[52] *See* Exec Order No.13,722, 81 Fed. Reg. 14,943, 14,943–44 (Mar. 15, 2016) (providing an example of an executive order related to North Korea that provided for the blocking of parties who "have engaged in significant activities undermining cybersecurity through the use of computer networks or systems against targets outside of North Korea" as well as other activities , including "censorship," "exportation of workers from North Korea," "abuse or violation of human rights," and those who "have sold, supplied, transferred, or purchased, directly or indirectly . . . metal, graphite, coal, or software, where any revenue or goods received may benefit the Government of North Korea or the Workers' Party of Korea").

[53] Press Release, U.S. Dep't of the Treasury, *supra* note 38 ("As cyber criminals use increasingly sophisticated methods and technology, we are committed to using the full range of measures, to include sanctions and regulatory tools, to disrupt, deter, and prevent ransomware attacks." (quoting U.S. Department of the Treasury Secretary Janet L. Yellen)).

pay ransoms.[54] U.S. authorities might also be able to recoup some ransomware payments, thereby depriving those cyber actors of resources while still allowing a speedy resumption of normal activities.[55] It has been posited that a blanket ban on ransomware payments would disproportionately affect smaller businesses "large enough to have something worth stealing but small enough to not have world-class infosec talent on staff."[56] The immediate potential for disruption—which might include disruption to vitally important infrastructure, as was the case with the Colonial Oil Pipeline—must be weighed seriously against the potential long-term deterrent effect a ban would seek to achieve.[57]

Moreover, a blanket ban would be merely one step in dissuading ransomware attacks. Such a blanket prohibition must be accompanied by enforcement to be truly effective. Government commitment to enforcement of a comprehensive ban might be lacking, for either reasons of resources or optics.[58] Companies' choosing to make illegal ransomware payments in violation of a ban could also result in the potential for extortion from ransomware attackers.[59]

---

[54] *See, e.g.,* Jacob Bunge, *JBS Paid $11 Million to Resolve Ransomware Attack*, WALL ST. J., https://www.wsj.com/articles/jbs-paid-11-million-to-resolve-ransomware-attack-11623280781 [https://perma.cc/ZBE8-3HDJ] (June 9, 2021) (providing an example of a company that paid a ransom "to avoid more disruptions"); Michael D. Shear, Nicole Perlroth & Clifford Krauss, *Colonial Pipeline Paid Roughly $5 Million in Ransom to Hackers*, N.Y. TIMES, https://www.nytimes.com/2021/05/13/us/politics/biden-colonial-pipeline-ransomware.html [https://perma.cc/3EMR-R8RW] (June 7, 2021) (same).

[55] David Uberti & Maria Armental, *DOJ Sees Crypto Seizures as a Priority in Anti-Ransomware Push*, WALL ST. J. (Oct. 12, 2021), https://www.wsj.com/articles/doj-sees-crypto-seizures-as-a-priority-in-anti-ransomware-push-11634072878 [https://perma.cc/VC6P-BU8T] ("The Justice Department is increasingly trying to claw back ransomware payments made by hacked companies . . . . Ramping up seizures is a key prong of the U.S. strategy to slow a spate of ransomware attacks that the White House has labeled a top national security threat . . . ." (citing Leo Tsao, principal deputy chief of the Department of Justice's money laundering and asset recovery section)).

[56] Tarah Wheeler & Ciaran Martin, *Should Ransomware Payments Be Banned?*, BROOKINGS INST. (July 26, 2021), https://www.brookings.edu/techstream/should-ransomware-payments-be-banned/ [https://perma.cc/8WQS-PDST].

[57] *See, e.g.*, Jason Breslow, *How to Stop Ransomware Attacks? 1 Proposal Would Prohibit Victims From Paying Up*, NPR (May 13, 2021), https://www.npr.org/2021/05/13/996299367/how-to-stop-ransomware-attacks-1-proposal-would-prohibit-victims-from-paying-up [https://perma.cc/7YDG-P6PW] ("[B]ecause ransomware is motivated by profit, a ban on payments would help choke off a prime driver of attacks. . . . On the other hand . . . there's a risk that a ban might only make the threat more pernicious." (citing a "public-private task force composed of members from Amazon Web Services, Microsoft, the FBI and the Secret Service, among others")).

[58] Wheeler & Martin, *supra* note 56 ("Even if ransomware payments were banned, it is difficult to imagine such a law being enforced: What prosecutor would seek to imprison hospital executives or trucking companies for paying off criminals in order to save lives and transport food?").

[59] Maggie Miller, *Top FBI Official Advises Congress Against Banning Ransomware Payments*, THE HILL (July 27, 2021), https://thehill.com/policy/cybersecurity/565110-top-fbi-official-advises-congress-against-banning-ransomware-payments [https://perma.cc/Z5Q3-ACGC] (quoting Bryan Vorndran, assistant director of the FBI's Cyber Division).

Alternative solutions to the ransomware crisis besides a blanket ban have certainly been proposed.[60] For example, Professor Westbrook has envisioned "a safe harbor for ransomware payment[s]" that would also serve to prevent attacks and enable their interdiction.[61] Other scholars have called for a treaty that would facilitate investigation and enforcement by international cooperation.[62]

Justifications for or alternatives to continuing to permit payments to malicious cyber actions, however, do not erase the fact that such payments are fundamentally at odds with the purposes of the U.S. sanctions regime. If federal legislators decide against enacting a ban on ransomware payments, they must do so while recognizing that the lack of such a ban undermines the essential purpose of the OFAC regulatory scheme by leaving a gap with respect to the prohibition of such payments.

CONCLUSION

A ban on the making of ransomware payments would certainly align with the intent of the U.S. sanctions regulations and remedy a notable shortcoming of that regulatory structure. The use of the SDN List to deal with those seeking ransoms creates a problem essentially of timing; while an attacker certainly might be one that would be named to the SDN List as a result of a cyberattack, the perpetrator may not be identified and designated until after that cyberattack has occurred. While OFAC encourages the prompt reporting of cyberattacks to the agency, the lag in timing may still permit ransom payments to be made to

---

[60] *See, e.g.*, Cynthia Brumfield, *Four States Propose Laws to Ban Ransomware Payments*, CSO ONLINE (June 28, 2021), https://www.csoonline.com/article/3622888/four-states-propose-laws-to-ban-ransomware-payments.html [https://perma.cc/U5TF-WSP8] ("A better alternative to banning ransom payments is requiring companies to report ransomware attacks to a central authority . . . ."); SIMON HANDLER, EMMA SCHROEDER, FRANCES SCHROEDER & TREY HERR, ATL. COUNCIL, COUNTERING RANSOMWARE: LESSONS FROM AIRCRAFT HIJACKING 6 (2021), https://www.atlanticcouncil.org/wp-content/uploads/2021/08/IB-RANSOMWARE-3.pdf [https://perma.cc/7A2J-9SY7] ("The United States and its allies should strive to empower companies to make choices that improve the security ecosystem without sacrificing their own interests. This includes helping to reveal more securely designed and supported products in the marketplace, enhancing the efficiency and efficacy of risk-transfer mechanisms like (but hardly limited to) cyber insurance, and markedly reducing the friction of operational collaboration between these victims' vendor companies and state law-enforcement agencies."); Bruce Schneier & Nicholas Weaver, *How to Cut Down on Ransomware Attacks Without Banning Bitcoin*, SLATE (June 17, 2021), https://slate.com/technology/2021/06/banning-cryptocurrencies-bitcoin-ransomware-disruption-exchanges.html [https://perma.cc/GU4B-WKRH] (suggesting "disrupt[ion of] the cryptocurrency markets" and "[m]aking them harder to use" as an alternative to banning Bitcoin entirely as a way to reduce ransomware attacks).

[61] *See* Amy Deen Westbrook, *A Safe Harbor for Ransomware Payments: Protecting Stakeholders, Hardening Targets, and Defending National Security*, 18 N.Y.U. J.L. & BUS. (forthcoming 2022) (manuscript at 392), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3899370 [https://perma.cc/ME2W-ZKZA].

[62] Oona A. Hathaway et al., *The Law of Cyber-Attack*, 100 CALIF. L. REV. 817, 822 (2012).

first-time or not-yet-identified cyber attackers. Without a supplemental blanket ban on ransomware payments in place, these undesignated attackers will be allowed to receive ransomware payments, even though the purpose of the malicious cyber-related activities sanctions programs is to prevent these sorts of actors from dealings in property with a U.S. nexus.

Preferred citation: Christine Abely, *Ransomware, Cyber Sanctions, and the Problem of Timing*, 63 B.C. L. REV. E. SUPP. I.-47 (2022), http://lawdigitalcommons.bc.edu/bclr/vol63/iss9/14/.