NEW YORK UNIVERSITY
JOURNAL OF LAW & BUSINESS

VOLUME 18 SPRING 2022 NUMBER 2

A SAFE HARBOR FOR RANSOMWARE PAYMENTS: PROTECTING STAKEHOLDERS, HARDENING TARGETS, AND DEFENDING NATIONAL SECURITY

AMY DEEN WESTBROOK*

Ransomware attacks have become common. Victims range from small municipalities to non-profits to giant multi-national corporations. These attacks disable the victim's cyber-systems and may result in financial losses, data leaks, business failures, and, in some cases, even loss of life. The hackers may be lone actors or infamous cyber-gangs; they may be hostile foreign countries or non-state actors such as terrorist groups.

Most victims pay the ransom. But payment does not guarantee the recovery of data as promised. In addition, payment transfers value to criminals and may jeopardize national security.

In an effort to cut off financial flows to the hackers, several U.S. agencies have targeted ransomware payments. Both the Office of Foreign Assets Control (OFAC) and the Financial Crimes Enforcement Network (FinCEN) have issued advisories emphasizing the potential liability for ransomware victims (and those assisting them) who pay prohibited persons or transmit funds without the required procedures.

* Kurt M. Sager Memorial Distinguished Professor of International and Commercial Law, Co-Director, Business and Transactional Law Center, Washburn University School of Law. I am grateful to David A. Westbrook for his comments, to Marcos Mendoza for his insurance law expertise, and to Perry Alexander, Robert Goldman, and John Symons for their guidance on technology questions. Thank you to my colleagues at the Central States Law Schools Association 2021 Annual Scholarship Conference for their suggestions on an earlier draft of this article. Thank you also to Alyssa Crenshaw and Tymber Long for their research assistance. All mistakes are, of course, my own.

This Article argues that the threat of legal liability for ransomware victims who pay the ransom, with no positive incentive, is unlikely to improve cybersecurity or even to stop payments. In fact, such threats may be counterproductive if they lead victims to conceal attacks. Instead, this article suggests the creation of a safe harbor for ransomware payment that (i) enables the victim and those who assist the victim to pay when necessary (protecting stakeholders), but that also (ii) deters attacks (hardening targets) and (iii) facilitates interdiction of attacks that do occur (defending national security).

Introduction

Imagine a nurse working an overnight shift. When the nurse enters an elderly patient's room to administer medication, the hospital laptop needed to confirm the correct medication shows only one message: "Your computer has been infected with a virus. Click here to resolve this issue." Clicking does not resolve the issue. All hospital computers display the

same message. The hospital initiates its required security incident response procedures[1] and shifts into crisis mode.

Hospital administrators soon receive a ransom demand: if a hefty sum in bitcoin[2] is paid to a specified pseudonymous address,[3] the hospital's computer system will be restored to operability. The hospital reacts swiftly, engaging a digital forensics and incident response company, calling its insurance company, and informing regulators and law enforcement. With every passing minute, however, patient care may be compromised and sensitive data may be stolen. The hospital pays the ransom, receives the decryption key, and starts work to resume normal operations.

In an increasingly digital world, security is often breached digitally. Reliable statistics on ransomware are difficult to generate but, according to some reports, 43% of European and North American firms were targeted by cybercriminals in 2020 and, of those, one in six involved a ransom demand.[4] In the United States, 71% of targeted companies paid the ransom.[5] Experts estimate that ransomware hackers extracted over $400

---

1. 45 C.F.R. §§ 164.304, 164.308(a)(6) (2021) (defining "security incident" and identifying requirements for implementing security incident procedures in regulations promulgated pursuant to the Health Insurance Portability and Accountability Act).

2. Bitcoin is both a cryptocurrency and a protocol, so in this article "Bitcoin" (with an uppercase letter B) is used to label the protocol, software and community, and "bitcoin" (with a lowercase letter b) is used to label units of cryptocurrency.

3. *See* discussion *infra* Section II.D. A Bitcoin address, for example, is represented by a 26-35-character alphanumeric string that indicates the virtual location to which Bitcoin are sent and received. Aff. Supp. Appl. for Seizure Warrant, No. 3:21-mj-70945-LB, ¶ 18 (N.D. Cal. June 7, 2021), https://www.justice.gov/opa/press-release/file/1402056/download (defining Bitcoin addresses).

4. Hiscox, Hiscox Cyber Readiness Report 2021: Don't Let Cyber Be a Game of Chance 2, (2021), https://www.hiscoxgroup.com/sites/group/files/documents/2021-04/Hiscox%20Cyber%20Readiness%20Report%202021.pdf (reporting results of survey of 6,042 companies in eight countries). *See also* Martin Croucher, *Almost Half Of Firms Hit By Cyberattack In 2020, Report Says*, Law360 (Apr. 20, 2021, 2:22 PM), https://www.law360.com/articles/1376896/almost-half-of-firms-hit-by-cyberattack-in-2020-report-says (discussing a recent Hiscox, Ltd. report).

5. Hiscox Cyber Readiness Report 2021, *supra* note 4, at 10 (calling the United States the "most fruitful territory for the ransom specialists"). *See also* Daniel Silver et al., *Gov't Authorities Should Assist Ransomware Targets*, Law360 (May 21, 2021, 5:47 PM), https://www.law360.com/articles/1386039/gov-t-

million in 2020.[6] Most of these ransoms were paid to pseudonymous addresses in cryptocurrencies—also known as convertible virtual currencies—such as Bitcoin.

For the hospital, however, paying the ransom is not the end of the story. The hospital, the incident response company, the insurance company, and the hospital's bank may now face investigations and liability for the hospital's ransomware payment. In their efforts to combat the rising tide of ransomware attacks, regulators are threatening enforcement actions against victims who pay ransoms–as well as those who assist them.

Few entities, faced with a ransomware attack, can afford to refuse the hackers' terms. Not paying the ransom may result in financial ruin or even loss of life.[7] In circumstances presenting the threat of significant harm, and in the absence of feasible alternatives, paying the ransoms is ethically justifiable.[8] At any rate, and, as noted above, at least in the United States, most corporate victims pay the ransom.[9]

---

authorities-should-assist-ransomware-targets (asserting that most companies pay ransomware ransoms).

6. CHAINALYSIS, RANSOMWARE 2021: CRITICAL MID-YEAR UPDATE 3, (2021), https://go.chainalysis.com/rs/503-FAP-074/images/Ransomware-2021-update.pdf (noting that $400 million is likely less than the true total).

7. John Reed Stark, *An OFAC Compliance Checklist For Ransomware Payments*, LAW360 (Feb. 2, 2021, 5:43 PM), https://www.law360.com/articles/1349647/ (identifying potential consequences for not paying a ransom). A ransomware attack against a hospital in Germany in 2020 reportedly led to the diversion of an emergency room patient to another hospital and a delay in treatment of over an hour. The patient died. *See* Dan Goodin, *A Patient Dies After Ransomware Attack Hits a Hospital*, WIRED (Sept. 19, 2020, 8:00 AM), https://www.wired.com/story/a-patient-dies-after-a-ransomware-attack-hits-a-hospital/ (reporting that German authorities were seeking the ransomware perpetrators on suspicion of negligent manslaughter). *But see* Patrick Howell O'Neill, *Ransomware Did Not Kill a German Hospital Patient*, MIT TECH. REV. (Nov. 12, 2020), https://www.technologyreview.com/2020/11/12/1012015/ransomware-did-not-kill-a-german-hospital-patient/ (reporting that authorities determined the patient was in such poor health that she likely would have died anyway).

8. *Should Cities Ever Pay Ransom to Hackers?*, WALL ST. J. (Sept. 17, 2019, 10:02 PM), https://www.wsj.com/articles/should-cities-ever-pay-ransom-to-hackers-11568772120?mod=article_inline (quoting Craig Shue).

9. John Reed Stark, *Ransomware's Dirty Little Secret: Most Corporate Victims Pay*, LINKEDIN (Jan. 28, 2019), https://www.linkedin.com/pulse/ransomwares-dirty-little-secret-most-victims-pay-john-reed-stark/ (comparing the payment of ransomware with the frequency of paying an electric bill).

Paying a ransom can only be ethically justified, however, as the best among bad alternatives. Payment is likely to incentivize hackers to attack other targets.[10] To make matters worse, paying the ransom may not lead to recovery of the data as promised.[11] Paying ransoms, by definition, transfers value to criminals, and that is against many laws.

But more than simple illegality is at issue. While ransomware hackers may be lone criminals or infamous cybergangs, they may also be hostile foreign countries, or non-state actors such as terrorist groups. Ransomware hackers have been identified in several jurisdictions, including North Korea,[12] Iran,[13] Russia[14] and China,[15] which raises security concerns for the United States. Ransomware and other digital threats tend

---

10. *Should Cities Ever Pay Ransom to Hackers?*, *supra* note 8 (quoting Frank Cilluffo).

11. FED. BUREAU OF INVESTIGATION, INTERNET CRIME REPORT 2020, at 14 (Mar. 17, 2021), https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf (noting that payment may not restore a victim's data).

12. U.S. DEP'T OF TREASURY ET AL., DPRK CYBER THREAT ADVISORY: GUIDANCE ON THE NORTH KOREAN CYBER THREAT (Apr. 15, 2020) https://home.treasury.gov/system/files/126/dprk_cyber_threat_advisory_20200415.pdf (alleging North Korea has been responsible for a number of high-profile cyberattacks).

13. In 2018, two Iranians were indicted in connection with the SamSam ransomware attack. Indictment, United States v. Savandi, No. 2016R00103 (D. N.J. Nov. 26, 2018), https://www.justice.gov/opa/press-release/file/1114741/download. *See* U.S. DEP'T OF JUST., TWO IRANIAN MEN INDICTED FOR DEPLOYING RANSOMWARE TO EXTORT HOSPITALS, MUNICIPALITIES, AND PUBLIC INSTITUTIONS, CAUSING OVER $30 MILLION IN LOSSES (Nov. 28, 2018), https://www.justice.gov/opa/pr/two-iranian-men-indicted-deploying-ransomware-extort-hospitals-municipalities-and-public.

14. *See To Stop the Ransomware Pandemic, Start with the Basics*, ECONOMIST (Jun. 19, 2021), https://www.economist.com/leaders/2021/06/19/to-stop-the-ransomware-pandemic-start-with-the-basics (reporting that Russia provides sanctuary to cyber attackers).

15. *See* Ben Kochman & Stewart Bishop, *US, Allies Say China Behind Massive Microsoft Server Attack*, LAW360 (July 19, 2021, 4:24 PM), https://www.law360.com/articles/1404209/us-allies-say-china-behind-massive-microsoft-server-attack (reporting White House claims that hackers affiliated with the Chinese government have hit private companies with ransomware); *America under Cyber Siege: Preventing and Responding to Ransomware Attacks: Hearing Before the Comm. on the Judiciary*, 117th Cong. 3 (2021) (statement of Deputy Assistant Att'y Gen. Richard Downing), https://www.judiciary.senate.gov/imo/media/doc/Downing%20-%20Statement.pdf (discussing charges against hackers in China operating on behalf of its Ministry of State Security) [hereinafter statement of Downing].

to be invisible until realized, which amplifies the potential to compromise U.S. critical infrastructure.[16] In August 2021, President Biden labeled cybersecurity the "core national security challenge" for the United States.[17]

Unlike conventional warfare or cross-border crime, there are few international legal norms to help contain cyberattack risk.[18] Ransomware attacks are difficult to combat because the threat is everywhere, and nowhere, until the attack occurs. Victims range from small municipalities to non-profits to multinational corporations and governments.[19] Ransomware "blurs the boundaries between state and private actors and between geopolitics and crime,"[20] and the law is struggling to respond.

Strategically significant economic transactions have long been highly regulated. In particular, regulators have long sought to safeguard national security by monitoring and controlling payments. In the wake of the September 11th attacks, the discovery and prevention of terrorist financing became a key pillar of U.S. security architecture.[21] Perhaps unsurprisingly, paying a ransom and thereby aiding the "enemy" may trigger costly government investigations and penalties.[22] Regulators have threatened enforcement of sanctions and anti-money laundering laws not only against ransomware victims

16. *See* discussion *infra* Sections III.A and III.B (describing, for example, the ransomware attack against Colonial Pipeline).

17. Dustin Volz & David Uberti, *Biden Says Cybersecurity Is the 'Core National Security Challenge' at CEO Summit*, WALL ST. J. (Aug. 25, 2021), https://www.wsj.com/articles/biden-to-hold-cybersecurity-summit-with-tech-giants-top-banks-energy-firms-11629882002 (reporting that Biden urged the private sector representatives at the meeting to raise the bar, and emphasized their shared responsibilities).

18. *See To Stop the Ransomware Pandemic, Start with the Basics*, *supra* note 14 (reporting that there is novelty and confusion in the geopolitical cyber-domain regarding legal norms).

19. *See* discussion *infra* Section II.B.

20. *To Stop the Ransomware Pandemic, Start with the Basics*, *supra* note 14 (discussing why dealing with cyber-insecurity is hard).

21. *See* USA Patriot Act, Pub. L. No. 107-56, 115 Stat. 272 (2001). *See also* U.S. DEP'T OF TREASURY, 2003 NATIONAL MONEY LAUNDERING STRATEGY, at 4 (Nov. 18, 2003), https://www.treasury.gov/press-center/press-releases/Documents/js10102js1010.pdf (explaining that the Act enhanced communications within and between the Federal government and financial institutions regarding the financial funding of terrorists).

22. John Reed Stark, *supra* note 7 (identifying potential government action if a victim pays the ransomware).

who pay, but also against third-party service providers who facilitate payments. On October 1, 2020, the Department of the Treasury's Financial Crimes Enforcement Network (FinCEN) bureau warned banks, incident response companies, and cyber insurance companies of potential anti-money laundering liability connected with assisting ransomware victims with ransom payments.[23] FinCEN updated its advisory on November 8, 2021, emphasizing that ransomware payments require immediate attention from financial institutions.[24] The Department of the Treasury's Office of Foreign Assets Control (OFAC) warned companies on October 1, 2020 that OFAC adopts a strict liability sanctions enforcement policy against persons who, even unknowingly, pay ransomware attackers on the government's list of Specially Designated Nationals and Blocked Persons (SDNs).[25] On September 21, 2021, OFAC updated its advisory to encourage victim reporting and improvement in cyber-security practices.[26] Other specialized anti-terrorism rules[27] may also impose liability for making a ransomware payment.

---

23. FIN. CRIMES ENF'T NETWORK, ADVISORY ON RANSOMWARE AND THE USE OF THE FINANCIAL SYSTEM TO FACILITATE RANSOM PAYMENTS, FIN-2020-A006 (Oct. 1, 2020), https://www.fincen.gov/sites/default/files/advisory/2020-10-01/Advisory%20Ransomware%20FINAL%20508.pdf.

24. FIN. CRIMES ENF'T NETWORK, ADVISORY ON RANSOMWARE AND THE USE OF THE FINANCIAL SYSTEM TO FACILITATE RANSOM PAYMENTS, FIN-2021-A004 (Nov. 8, 2021), https://www.fincen.gov/sites/default/files/advisory/2021-11-08/FinCEN%20Ransomware%20Advisory_FINAL_508_.pdf (updating the October 1, 2020, advisory).

25. OFF. OF FOREIGN ASSETS CONTROL, U.S. DEP'T OF TREASURY, ADVISORY ON POTENTIAL SANCTIONS RISKS FOR FACILITATING RANSOMWARE PAYMENTS, (Oct. 1, 2020), https://home.treasury.gov/system/files/126/ofac_ransomware_advisory_10012020_1.pdf.

26. OFF. OF FOREIGN ASSETS CONTROL, U.S. DEP'T OF TREASURY, UPDATED ADVISORY ON POTENTIAL SANCTIONS RISKS FOR FACILITATING RANSOMWARE PAYMENTS, (Sept. 21, 2021), https://home.treasury.gov/system/files/126/ofac_ransomware_advisory.pdf (updating the October 1, 2020, advisory); *see also Treasury Takes Action Against Suex: What You Need To Know*, CHAINALYSIS (Sept. 22, 2021), https://go.chainalysis.com/ofac-update-suex-recording.html?aliId=eyJpIjoiUURPXC9IbklWd0FjU3NTUDAiLCJ0IjoidWZzdWR5UG9qTGQxa3Z0RTcrcDNhZz09In0%253D (describing the reasons for the update).

27. *See* discussion *infra* Section III.D.

How do we steer between the Scylla of legal liability and the Charybdis of a cyberattack?[28] Sometimes, as in our hospital hypothetical, ransoms should be paid as the lesser evil. Simply punishing ransom payments, therefore, would be unjust and probably insufficient. Confronted with potential loss of life, people may rightly choose legal liability.

On the other hand, society cannot allow itself to be held hostage. Public order requires that those who endanger individual lives, enterprises, and core social functions be resisted, and that there be consequences for such endangerment. That is, the status quo, in which many enterprises simply pay off cybercriminals, incentivizes and facilitates more cyberattacks, and is, thereby, unsustainable.

The threat of legal liability for ransomware payments with no positive incentive for potential victims is unlikely to encourage adoption of sound security measures or even to stop payments, and may be counterproductive if it leads victims to conceal attacks. This article argues for the creation of a safe harbor for payment that (i) enables the victim and those who assist the victim to pay when necessary (protecting stakeholders), but that also (ii) deters attacks (hardening targets), and (iii) facilitates interdiction of attacks that do occur (defending national security). Part II of this Article reviews the current ransomware landscape, including the ransomware hackers, their weapons, and the mechanics of such attacks. Part III examines the national security implications of ransomware attacks, and the liabilities that payment of a ransom may trigger. Part IV looks at the decision to pay a ransom and the practical and ethical considerations that ransomware victims currently confront. In response to the public and private dilemmas now presented by ransomware attacks, Part V proposes a safe harbor: a system of clear requirements and regulatory restraint designed to contain and manage ransomware threats with the minimum individual and societal cost.

---

28. *See* Edward J. Krauland et al., *Five Key Takeaways from OFAC and FinCEN's Ransomware Advisories*, LEXOLOGY: INTERNATIONAL COMPLIANCE BLOG (Oct. 6, 2020), https://www.lexology.com/library/detail.aspx?g=631463e7-9bad-4d95-a92c-a1af3d874e46 (describing the "conundrum" faced by ransomware victims and companies that assist them).

I.
RANSOMWARE ATTACKS

A. *What Is Ransomware?*

1. *Definition*

Malicious computer software, or "malware," is intended to cause a victim's computer to behave in a manner inconsistent with the intention of the owner or user of the victim's computer, often unbeknownst to that person.[29] "Ransomware" is a species of malware that "infects a computer and encrypts some or all of the data or files on the computer, and then demands that the victim pay a ransom in order to decrypt and recover the files, or in order to prevent the hacker from distributing or destroying the data."[30] A ransomware attack may take a variety of forms, but often involves either a "locker" or a "crypto" strategy. "Locker" ransomware holds the user's data behind a locked interface, demanding that the victim pay the ransom to unlock the data.[31] Under such an attack, a computer may be unusable, but data files may be untouched.[32] "Crypto" ransomware leaves the data accessible to the system but makes it indecipherable and therefore unusable without the decryption key.[33] During a crypto attack, the computer may still be usable, though continuing to use it may spread the ransomware.[34]

---

29. Indictment at 28, United States v. Hyok, No. CR 2:20-cr-00614-DMG (C.D. Cal. Dec. 8, 2020) (defining the term).

30. *Id.* at 30 (defining the term).

31. *See* KEVIN SAVAGE ET AL., SYMANTEC, THE EVOLUTION OF RANSOMWARE 6 (2015), https://its.fsu.edu/sites/g/files/imported/storage/images/information-security-and-privacy-office/the-evolution-of-ransomware.pdf (outlining security responses to ransomware).

32. *See id.*

33. *See id.*

34. *See* Alison Grace Johansen, *What is a Computer Virus?*, NORTON (July 23, 2020), https://us.norton.com/internetsecurity-malware-what-is-a-computer-virus.html (warning that "once the virus infects your computer, the virus can infect other computers on the same network); *see also* Tyler Omoth, *How Computer Viruses Spread and How to Avoid Them*, ITPRO (Mar. 26, 2021), https://www.itpro.com/security/malware/357313/how-do-computer-viruses-spread (pointing out that once "you're alerted to the presence of a virus, you need to remove it as soon as possible. The longer you leave it the more damage it can do.").

2. *History*

One of the first widely known ransomware attacks occurred in 1989. Biologist Joseph Popp distributed 20,000 infected disks labeled, "AIDS Information – Introductory Diskettes" to AIDS researchers.[35] Once the recipient's computer was booted up 90 times, the AIDS Trojan virus hid or encrypted the computer's files.[36] In order to regain access, users were instructed to send $189 to PC Cyborg Corporation in Panama.[37] Popp did not make much of a profit from his virus because of the difficulty in sending the payments and the development of antidote tools; he was arrested and charged with blackmail in the United Kingdom.[38]

The use of ransomware that encrypted users' data and extorted some kind of payment began to gain steam in the mid-2000s;[39] locker ransomware, in particular, became popular in the late 2000s.[40] Some examples of more recent ransomware

35. Juliana De Groot, *A History of Ransomware Attacks: The Biggest and Worst Ransomware Attacks of All Time,* DIGITAL GUARDIAN (Dec. 1, 2020), https://digitalguardian.com/blog/history-ransomware-attacks-biggest-and-worst-ransomware-attacks-all-time.

36. Kaveh Waddell, *The Computer Virus that Haunted Early AIDS Researchers*, THE ATLANTIC (May 10, 2016), https://www.theatlantic.com/technology/archive/2016/05/the-computer-virus-that-haunted-early-aids-researchers/481965/ (detailing the AIDS Trojan virus).

37. Marlese Lessing, *Case Study: AIDS Trojan Ransomware,* SDXCENTRAL (Jun. 3, 2020), https://www.sdxcentral.com/security/definitions/case-study-aids-trojan-ransomware/ (explaining how the virus worked).

38. Waddell, *supra* note 36 (explaining the payment instructions).

39. *See* Savage, *supra* note 31, at 9 (discussing the Trojan.Gpcoder and Trojan.Cryzip families of viruses).

40. *See id.* at 10 (discussing the Trojan.Randsom.C malware).

strains[41] have included: CryptoLocker,[42] SamSam,[43] Emotet,[44] Petya and NotPetya,[45] WannaCry,[46] and DarkSide.[47]

The pace of ransomware attacks has continued to accelerate, breaking records in 2020 and 2021 with the United States bearing the brunt.[48] One factor contributing to the number of

---

41. Emsisoft Malware Lab, *Ransomware Statistics for 2021: Q2 Report,* EMSISOFT BLOG (July 6, 2021), https://blog.emsisoft.com/en/38864/ransomware-statistics-for-2021-q2-report/ (noting that STOP (Djvu) attacks accounted for 71.20% of ransomware strains in the second quarter of 2021); *see also Ransomware Attacks and Types – How Encryption Trojans Differ,* KASPERSKY, https://usa.kaspersky.com/resource-center/threats/ransomware-attacks-and-types (last visited Aug. 2, 2021) (listing other variants including Bad Rabbit, Ryuk, Shade/Troldesh, Jigsaw, Petya, GoldenEye, GandCrab, B0r0nk0k, Dharma Brr, FAIRRANSOMWARE, and MADO).

42. CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY, ALERT TA13-309A, CRYPTOLOCKER RANSOMWARE INFECTIONS (Oct. 7, 2016), https://us-cert.cisa.gov/ncas/alerts/TA13-309A (explaining that CryptoLocker restricts access to infected computers and demands the victim provide a payment to the attackers to decrypt and recover their files); *see also* Bart Custers et al., *Laundering the Profits of Ransomware: Money Laundering Methods for Vouchers and Cryptocurrencies,* 28 EUR. J. CRIME, CRIM. L. & CRIM. JUST. 121, 132 (2020) (explaining that CryptoLocker was targeted at Microsoft Windows and is disseminated via infected email attachments).

43. Cybersecurity & Infrastructure Security Agency, Alert AA18-337A, SAMSAM RANSOMWARE (Dec. 3, 2018), https://us-cert.cisa.gov/ncas/alerts/AA18-337A (warning that, once in, the ransomware infects all reachable hosts on the victim's network).

44. CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY, ALERT TA18-201A, EMOTET RANSOMWARE (Jan. 23, 2020), https://us-cert.cisa.gov/ncas/alerts/TA18-201A (explaining that Emotet is a modular banking Trojan affecting state, local, tribal, and territorial governments, and the private and public sectors).

45. CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY, ALERT TA17-181A, PETYA RANSOMWARE (Feb. 15, 2018), https://us-cert.cisa.gov/ncas/alerts/TA17-181A (explaining that NotPetya is a variant of Petya attributed to the Russian military that encrypts files and makes Windows computers unusable).

46. *What is Wannacry/Wannacryptor?,* NAT'L CYBERSECURITY & COMMC'N. INTEGRATION CTR., https://us-cert.cisa.gov/sites/default/files/FactSheets/NCCIC%20ICS_FactSheet_WannaCry_Ransomware_S508C.pdf (last visited July 21, 2021).

47. CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY, ALERT AA21-131A, DARKSIDE RANSOMWARE: BEST PRACTICES FOR PREVENTING BUSINESS DISRUPTION FROM RANSOMWARE (July 8, 2021), https://us-cert.cisa.gov/ncas/alerts/aa21-131a (discussing Ransomware-as-a-Service).

48. Silver, *supra* note 5; Claudia Glover, *Unprecedented Ransomware Spike Puts Government in the Crosshairs,* TECHMONITOR (Aug. 4, 2021), https://techmonitor.ai/technology/cybersecurity/record-breaking-ransomware-at-

attacks in 2020 was the COVID-19 pandemic,[49] which shifted a substantial part of the U.S. workforce to working from home.[50] One survey found that, during the pandemic, over a third of companies did not practice common cybersecurity protocols such as phishing training and multi-factor authentication.[51] Remote work required people to do business from out-of-network, relatively unsecured, computers.[52] A computer network is only as strong as its least vigilant user,[53] and during the pandemic many users were overstretched and distracted.[54] But ransomware was a problem before 2020, and will continue to

---

tempt-spike (noting that the number of attempted attacks had already exceeded the total number for 2020).

49. FIN. CRIMES ENF'T NETWORK, ADVISORY ON CYBERCRIME AND CYBER-ENABLED CRIME EXPLOITING THE CORONAVIRUS DISEASE 2019 (COVID-19) PANDEMIC, FIN-2020-A005 (July 30, 2020), https://www.fincen.gov/sites/default/files/advisory/2020-07-30/FinCEN%20Advisory%20Covid%20Cybercrime%20508%20FINAL.pdf (warning that illicit actors were engaged in fraudulent schemes that exploited vulnerabilities created by the pandemic); *To Stop the Ransomware Pandemic, Start with the Basics*, ECONOMIST (June 19, 2021), https://www.economist.com/leaders/2021/06/19/to-stop-the-ransomware-pandemic-start-with-the-basics (noting that workers logging in from home added to cyber-risk).

50. Robert McMillan et al., *NYC's Subway Operator and Martha's Vineyard Ferry Latest to Report Cyberattacks,* WALL ST. J. (June 2, 2021), https://www.wsj.com/articles/ransomware-scourge-continues-as-essential-services-are-hit-11622672685 (stating that the potential profit from ransomware coupled with the increase in remote working during COVID-19 provided the incentive and opportunity for ransomware); Ben Kochman, *Insurers Set Limits on Risky Sectors Amid Cybercrime Spike*, LAW360 (May 21, 2021), https://www.law360.com/articles/1387175/insurers-set-limits-on-risky-sectors-amid-cybercrime-spike (noting that work from home environments created security gaps).

51. Sydney Wess, *Cybersecurity Risk Management Best Practices,* VISUAL OBJECTS (Oct. 27, 2020), https://visualobjects.com/app-development/blog/cybersecurity-risk-management (providing statistics regarding cybersecurity measures companies required for remote work during COVID-19).

52. Michael K. Lindsey, *Cybersecurity Concerns for 2021,* 63-FEB ORANGE COUNTY LAW. 34 (Feb. 2021), http://www.virtualonlineeditions.com/publication/?m=15276&i=692099&view=articleBrowser&article_id=3884376&ver=html5 (noting that people's home Wi-Fi networks may not be up to the standards of protection maintained in a company office).

53. *Id.* (explaining that the bulk of data breaches are due to human error).

54. Ben Kochman, *How Ransomware Will Continue Wreaking Havoc In 2021*, LAW360 (Jan. 3, 2021), https://www.law360.com/articles/1334799/how-ransomware-will-continue-wreaking-havoc-in-2021 (also noting communications gaps with remote employees).

challenge business and government actors in the coming years.

B. *Victims*

Ransomware victims encompass all kinds of entities, including health systems,[55] municipalities,[56] universities,[57] school districts,[58] and both large and small companies. The U.S. Federal Bureau of Investigation (FBI) reported that approximately 2,500 organizations were victims of ransomware in 2020.[59]

---

55. *See, e.g., 147,000 Patients Affected by Scripps Health Ransomware Attack,* HIPAA J. (June 3, 2021), https://www.hipaajournal.com/147000-patients-affected-by-scripps-health-ransomware-attack/ (detailing the attack).

56. For example, there was a coordinated attack on 22 Texas municipalities in 2019. *Should Cities Ever Pay Ransom to Hackers?,* WALL ST. J. (Sept. 17, 2019), https://www.wsj.com/articles/should-cities-ever-pay-ransom-to-hackers-11568772120 (featuring the comments of academic experts). The Texas attacks have been attributed to REvil. *US Justice Department Announces Indictment Against REvil Ransomware Suspect Behind 2019 Ransomware Attack on Texas Municipalities*, TEX. DEP'T OF INFO. RES. (Nov. 8, 2021), https://dir.texas.gov/news/us-justice-department-announces-indictment-against-revil-ransomware-suspect-behind-2019.

57. For example, in June 2020, the University of California paid over $1 million to salvage research locked down by ransomware. Charlie Osborne, *University of California SF Pays Ransomware Hackers $1.14 Million to Salvage Research,* ZDNET (June 30, 2020), https://www.zdnet.com/article/university-of-california-sf-pays-ransomware-hackers-1-14-million-to-salvage-research/ (discussing the measures undertaken by the university). That same summer, the University of Utah paid approximately half a million dollars to prevent ransomware hackers from leaking student data. Catalin Cimpanu, *University of Utah Pays $457,000 to Ransomware Gang,* ZDNET (Aug. 21, 2020), https://www.zdnet.com/article/university-of-utah-pays-457000-to-ransomware-gang/ (noting that the university restored much of their data from backups).

58. Tawnell D. Hobbs, *Schools Struggling to Stay Open Get Hit By Ransomware Attacks,* WALL ST. J (Nov. 13, 2020), https://www.wsj.com/articles/my-information-is-out-there-hackers-escalate-ransomware-attacks-on-schools-11605279160 (stating the newspaper documented nearly three dozen ransomware attacks on school districts between March and November 2020).

59. FED. BUREAU OF INVESTIGATIONS, *supra* note 11, at 14 https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf (noting those incidents triggered over $29 million in adjusted losses); *see also* Emsisoft Malware Lab, *The State of Ransomware in the U.S.: Report and Statistics 2020,* EMSISOFT BLOG (Jan. 18, 2021), https://blog.emsisoft.com/en/37314/the-state-of-ransomware-in-the-us-report-and-statistics-2020/ (estimating that approximately 2,400 U.S. entities suffered attacks in 2020).

Examples abound. In August 2019, the computers of 22 municipalities in Texas fell victim to a coordinated attack seeking $2.5 million to unlock their files.[60] In June 2020, the NetWalker hackers extorted $1.14 million from the University of California at San Francisco's School of Medicine[61] "in exchange for a tool to unlock the encrypted data and the return of the data they obtained."[62] In July 2020, the University of Utah paid unknown hackers over $450,000 in response to an attack on the computer services for the College of Social and Behavioral Science.[63] In May 2021, Scripps Hospital System in San Diego was struck by a ransomware attack which lasted nearly four weeks and affected over 147,000 patients.[64]

---

60. Bobby Allyn, *22 Texas Towns Hit with Ransomware Attack in 'New Front' of Cyberassault,* NPR (Aug. 20, 2019), https://www.npr.org/2019/08/20/752695554/23-texas-towns-hit-with-ransomware-attack-in-new-front-of-cyber-assault (reporting that the ransomware hackers requested a $2.5 million ransom); s*ee also* Amelia A. Boylan, *After the Ransomware Attacks: Texas Governance and Authorities for Cyberattack Response*, HOMELAND SECURITY TODAY (Nov. 13, 2019), https://www.hstoday.us/subject-matter-areas/infrastructure-security/after-the-ransomware-attacks-texas-governance-and-authorities-for-cyberattack-response/ (noting that the Sodinokibi ransomware strain was used).

61. Davey Winder, *The University of California Pays $1 Million Ransom Following Cyber Attack*, FORBES (June 29, 2020), https://www.forbes.com/sites/daveywinder/2020/06/29/the-university-of-california-pays-1-million-ransom-following-cyber-attack/?sh=623202f618a8. The NetWalker hackers were reported to be responsible for the University of California, San Francisco, hack in June 2020; *see* Joe Tidy, *How Hackers Extorted $1.14m from University of California, San Francisco*, BBC (June 29, 2020), https://www.bbc.com/news/technology-53214783 (claiming to have observed the ransom negotiation).

62. *See* Univ. of Cal. San Francisco, *Update on IT Security Incident at UCSF,* CAMPUS NEWS (June 26, 2020), https://www.ucsf.edu/news/2020/06/417911/update-it-security-incident-ucsf (discussing the hack); Lauren Berg, *Calif. University Says It Paid $1.14M in Ransomware Attack,* LAW360 (June 29, 2020) (reporting that the malware rendered a number of School of Medicine servers inaccessible).

63. Scott D. Pierce, *University of Utah Pays $450K to Stop Cyberattack on Servers,* U.S. NEWS (Aug. 22, 2020), https://www.usnews.com/news/best-states/utah/articles/2020-08-22/university-of-utah-pays-450k-to-stop-cyberattack-on-servers.

64. *147,000 Patients Affected by Scripps Health Ransomware Attack, supra* note 55 (noting that staff were forced to work with paper charts and the attackers acquired some patient information). It is unknown who is responsible. Kat Jercich, *Scripps CEO Says Attack Was Ransomware,* HEALTHCARE IT NEWS (May 26, 2021), https://www.healthcareitnews.com/news/scripps-ceo-says-attack-was-ransomware (noting that a number of recent attacks on healthcare institutions have involved Conti ransomware).

It is possible some non-profits and municipalities are softer targets because they may have weaker cybersecurity controls, including inadequate system backups and ineffective incident response capabilities.[65] Other attacks may be motivated by the potential for far-reaching impacts and maximum publicity. In May 2021, DarkSide encrypted Colonial Pipeline's data, which precluded operation of its business.[66] The ensuing shutdown of pipelines, which served much of the eastern United States, resulted in runs on gasoline, higher gas prices, and shortages[67] that impacted millions of Americans.[68] Colonial Pipeline paid $4.4 million in Bitcoin to DarkSide to regain control of its pipeline data.[69]

C. *Hackers and Their Weapons*

1. *Examples*

In some cases, the attackers are known to authorities; many are repeat players. DarkSide, which is said to operate from Russia, carried out a ransomware attack on the North American division of chemical distribution giant Brenntag[70]

---

65. FIN. CRIMES ENF'T NETWORK, *supra* note 24, https://www.fincen.gov/sites/default/files/advisory/2021-11-08/FinCEN%20Ransomware%20Advisory_FINAL_508_.pdf (citing the Multi-State Information Sharing and Analysis Center (MS-ISAC) security primer on ransomware published in 2020).

66. It also resulted in the theft of personal information of almost 6,000 employees and their families. Brian Fung, *Colonial Pipeline Says Ransomware Attack Also Led to Personal Information Being Stolen*, CNN (Aug. 16, 2021), https://www.cnn.com/2021/08/16/tech/colonial-pipeline-ransomware/index.html.

67. Collin Eaton & Amrith Ramkumar, *Colonial Pipeline Shutdown: Is There a Gas Shortage and When Will the Pipeline Be Fixed?*, WALL ST. J. (May 13, 2021), https://www.wsj.com/articles/colonial-pipeline-cyberattack-hack-11620668583 (noting that Colonial Pipeline supplied about 45% of the fuel consumed on the East Coast).

68. Abigail Ng, *A Major U.S. Pipeline Is Still Mostly Shut Due to a Cyberattack. Here's what you need to know*, CNBC (May 10, 2021), https://www.cnbc.com/2021/05/10/largest-us-fuel-pipeline-colonial-still-mostly-shut-impact-and-reopening.html (reporting that the pipeline connects Gulf Coast refineries with more than 50 million people in the U.S. South and East).

69. Approximately $2.3 million of the ransom was recovered by the Department of Justice (DOJ). *See* discussion *infra* Section V.F.

70. Lawrence Abrams, *Chemical Distributor Pays $4.4 Million to DarkSide Ransomware*, BLEEPINGCOMPUTER (May 13, 2021, 6:24 PM), https://www.bleepingcomputer.com/news/security/chemical-distributor-pays-44-

shortly before its attack on Colonial Pipeline. Brenntag reportedly also paid a $4.4 million ransom in Bitcoin to DarkSide in May 2021 to receive a decryptor and to prevent DarkSide from leaking exfiltrated data.[71] After the disruptions caused by the Colonial Pipeline attack, however, DarkSide apologized, stating "[o]ur goal is to make money, and not creating problems for society."[72] The group later took its website down, purportedly to avoid becoming part of the crossfire between the U.S. and Russian presidents.[73]

REvil (Ransomware Evil), also known as the Sodinokibi gang,[74] successfully carried out an attack against London foreign currency exchange firm Travelex on New Year's Eve in 2020, demanding a $6 million ransom.[75] REvil claimed to have accessed Travelex's network, downloading and encrypting its data.[76] After weeks of negotiations, Travelex agreed to pay a

---

million-to-darkside-ransomware (noting that DarkSide created a private leak page for the company with a description of the types of data that had been stolen and screenshots of some of the files).

71. *Id.* (noting that the $4.4 million in Bitcoin had been reduced from approximately $7.5 million initially demanded).

72. Tim Bradshaw & Hannah Murphy, *We Regret 'Creating Problems,' Say Colonial Petroleum Pipeline Hackers*, FIN. TIMES (May 10, 2021), https://www.ft.com/content/0afb53f0-f382-442a-9a32-02824ce8bb70 (reporting DarkSide claimed to be 'apolitical').

73. David E. Sanger, *Russia's Most Aggressive Ransomware Group Disappeared. It's Unclear Who Made That Happen.*, N.Y. TIMES (July 13, 2021), https://www.nytimes.com/2021/07/13/us/politics/russia-hacking-ransomware-revil.html?referringSource=articleShare (noting that some believe the group will reorganize under another name).

74. Some cybersecurity experts have highlighted a possible connection between DarkSide and REvil. *See DarkSide Ransomware Links to REvil Group Difficult to Dismiss,* FLASHPOINT (May 11, 2021), https://www.flashpoint-intel.com/blog/darkside-ransomware-links-to-revil-difficult-to-dismiss/ (suggesting that the DarkSide threat actors were from Russia, and likely former REvil affiliates); *What We Know About the DarkSide Ransomware and the US Pipeline Attack,* TREND MICRO (May 17, 2021, 3:25 AM), https://www.trendmicro.com/en_us/research/21/e/what-we-know-about-darkside-ransomware-and-the-us-pipeline-attac.html (noting that the DarkSide ransomware shared many similarities with REvil).

75. Akshaya Asokan, *Travelex Paid $2.3 Million to Ransomware Gang: Report*, BANK INFO SEC. (Apr. 10, 2020), https://www.bankinfosecurity.com/travelex-paid-23-million-to-ransomware-attackers-report-a-14094 (reporting that Travelex's customer service was crippled for weeks during the negotiations).

76. *Id.*

ransom in Bitcoin valued at $2.3 million.[77] Reporters at a UK newspaper claimed to have confirmed the payment with representatives of the Sodinokibi gang in an online chat.[78] In March 2021, REvil launched an attack against Taiwanese computer manufacturer Acer.[79] The Acer attack was reportedly accompanied by a $50 million ransom demand.[80] The technology news website *Bleeping Computer* reported that REvil offered Acer a 20% discount if the payment was transferred by an earlier deadline.[81] In May 2021, REvil launched a ransomware attack against meat producer JBS SA, and JBS's U.S. division paid the hackers a ransom in bitcoin valued at $11 million.[82] In early July 2021, REvil launched an attack on the Kaseya virtual system administrator[83] that infected hundreds of organizations worldwide, including both small and medium-sized companies (for whom ransoms in the $25,000–$150,000 range were reported) and larger service providers (one of which was reportedly asked for $5 million).[84]

---

77. *Id.*

78. *Id.* (reporting that the confirmation was claimed by the Journal).

79. Brittany Vincent, *Acer Falls Victim to $50 Million Ransomware Attack*, PC MAG (Mar. 20, 2021), https://www.pcmag.com/news/acer-falls-victim-to-50-million-ransomware-attack (speculating that REvil may have exploited a vulnerability in Microsoft Exchange to pull off the hack).

80. *Id.* (reporting that REvil threated to leak stolen data if the ransom went unpaid).

81. Lawrence Abrams, *Computer Giant Acer Hit by $50 Million Ransomware Attack*, BLEEPINGCOMPUTER (Mar. 19, 2021), https://www.bleepingcomputer.com/news/security/computer-giant-acer-hit-by-50-million-ransomware-attack/.

82. Jacob Bunge, *JBS Paid $11 Million to Resolve Ransomware Attack*, WALL ST. J. (June 9, 2021, 8:27 PM), https://www.wsj.com/articles/jbs-paid-11-million-to-resolve-ransomware-attack-11623280781 (explaining that JBS USA Holdings Inc. paid to avoid more disruptions in the nation's meat supply).

83. Robert McMillan, *Ransomware Attack Affecting Likely Thousands of Targets Drags On*, WALL ST. J. (July 4, 2021, 12:27 PM), https://www.wsj.com/articles/ransomware-group-behind-meat-supply-attack-threatens-hundreds-of-new-targets-11625285071 (explaining that REvil likely focused its attack on the Kaseya virtual system administrator, or VSA, software which is used by companies and technology service providers to carry out software updates on computer networks).

84. *Id.* (reporting that as many as 40,000 computers were affected worldwide). The abrupt disappearance of the group on July 13, 2021 reportedly left the then-current victims in the middle of negotiations to get their data back. David E. Sanger, *Russia's Most Aggressive Ransomware Group Disappeared. It's Unclear Who Made That Happen.* N.Y. TIMES (July 13, 2021), https://

Evil Corp., also known as the Dridex gang,[85] allegedly operates with the approval and possibly the assistance of the Russian Intelligence Services.[86] Evil Corp. has been active since 2007, and is blamed for using the Locky ransomware against individual households in 2016 as well as the BitPaymer ransomware against larger enterprise targets in 2017 and 2018.[87] Despite the fact that several of its members faced U.S. charges in 2019,[88] Evil Corp. went on to deploy WastedLocker in 2020, which attacked U.S. banks, financial institutions, and a number of corporations including Garmin.[89] In 2021, Evil Corp. likely deployed the Phoenix Locker ransomware against a vari-

---

www.nytimes.com/2021/07/13/us/politics/russia-hacking-ransomware-revil.html?referringSource=articleShare.

85. Lawrence Abrams, *New Evil Corp Ransomware Mimics PayloadBin Gang to Evade US Sanctions*, BLEEPINGCOMPUTER (June 6, 2021, 4:52 PM), https://www.bleepingcomputer.com/news/security/new-evil-corp-ransomware-mimics-payloadbin-gang-to-evade-us-sanctions/ (reporting that Evil Corp. also goes by Indrik Spider).

86. *See* Press Release, U.S. Dep't of the Treasury, Treasury Sanctions Russia with Sweeping New Sanctions Authority (Apr. 15, 2021), https://home.treasury.gov/news/press-releases/jy0127.

87. Catalin Cimpanu, *New WastedLocker Ransomware Demands Payments of Millions of USD*, ZDNET (June 23, 2020), https://www.zdnet.com/article/new-wastedlocker-ransomware-demands-payments-of-millions-of-usd/ (calling Evil Corp "one of the biggest malware operations on the planet").

88. Bobby Allyn, *Russian Hacking Group Evil Corp. Charged by Federal Prosecutors in Alleged Bank Fraud*, NPR (Dec. 5, 2019, 1:43 PM) https://www.npr.org/2019/12/05/785034567/russian-hacking-group-evil-corp-charged-by-federal-prosecutors-in-alleged-bank-f (reporting the criminal indictments of Maksim Yakubets and Igor Turashev, both of whom lived in Russia). The United States also offered a $5 million reward for information leading to the arrest of Yakubets. Lindsey O'Donnell, *Feds Offer $5M Reward to Nab 'Evil Corp' Dridex Hacker*, THREATPOST (Dec. 5, 2019, 12:55 PM), https://threatpost.com/feds-5m-reward-evil-corp-dridex-hacker/150858/. OFAC also imposed sanctions on Evil Corp. itself. Sanctions List Search for Evil Corp., OFF. OF FOREIGN ASSETS CONTROL, U.S. DEP'T OF THE TREASURY, https://sanctionssearch.ofac.treas.gov/Details.aspx?id=26664 (last visited Oct. 20, 2021) (listing Evil Corp.).

89. Alex Hern, *Ransomware Attack on Garmin Thought to Be the Work of 'Evil Corp'*, THE GUARDIAN (July 27, 2020), https://www.theguardian.com/technology/2020/jul/27/ransomware-attack-on-garmin-thought-to-be-the-work-of-evil-corp (reporting that Garmin had been held hostage for a reported $10 million ransom).

ety of targets, including U.S. commercial insurance giant CNA Financial Corp.[90]

2. *National/Political Motivations*

A number of attacks have been carried out by foreign governments or state-sponsored entities. The U.S. government has attributed both the 2014 Sony Pictures Entertainment hack and the 2017 WannaCry 2.0 ransomware attacks to North Korean state-sponsored cyber-crime activity (referred to as Hidden Cobra[91] or the Lazarus Group). An April 2020 cyber threat advisory issued by the FBI and U.S. Departments of State, Treasury, and Homeland Security warned that, under the pressure of U.S. and UN sanctions, North Korea is employing cybercrime to generate revenue for its weapons of mass destruction and ballistic missile programs, as well as to disrupt critical U.S. infrastructure.[92] One expert has warned that "threat actors associated with rival nations such as Iran and North Korea have adopted ransomware attacks as a fast and easy means to bypass U.S. economic sanctions and funnel badly needed capital into their cash-starved economies."[93]

In April 2021, President Biden signed an executive order blocking property of certain persons in response to the malicious cyberactivities of the Russian government.[94] The order included in particular the Russian intelligence services, while OFAC concurrently added over 40 persons in the Russian technology sector to the SDN list.[95] In the Treasury Department's

---

90. Elizabeth Montalbano, *Insurance Giant CNA Hit with Novel Ransomware Attack*, THREATPOST (Mar. 26, 2021, 12:06 PM), https://threatpost.com/cna-hit-novel-ransomware/165044/ (initially reporting that CNA planned to restore its systems using backup rather than pay the ransom).

91. U.S. DEP'T OF THE TREASURY, DPRK CYBER THREAT ADVISORY: GUIDANCE ON THE NORTH KOREAN CYBER THREAT (Apr. 15, 2020), https://home.treasury.gov/system/files/126/dprk_cyber_threat_advisory_20200415.pdf (reporting that Australia, Canada, New Zealand, and the United Kingdom joined the U.S. in attributing WannaCry 2.0 to the DPRK).

92. *Id.*

93. John Reed Stark, *An OFAC Compliance Checklist for Ransomware Payments*, LAW360 (Feb. 2, 2021, 5:43 PM), https://www.law360.com/articles/1349647/.

94. Exec. Order No. 14,024, 86 Fed. Reg. 20249 (Apr. 15, 2021).

95. OFF. OF FOREIGN ASSETS CONTROL, U.S. DEP'T. OF THE TREASURY, ISSUANCE OF EXECUTIVE ORDER BLOCKING PROPERTY WITH RESPECT TO SPECIFIED HARMFUL FOREIGN ACTIVITIES OF THE GOVERNMENT OF THE RUSSIAN FEDERA-

accompanying press release, it stated that Russian intelligence services executed a number of recent cyberattacks, including the 2020 SolarWinds cyberattack against some U.S. government targets.[96] The Treasury Department also stated that, to bolster their malicious cyber operations, Russian intelligence services "cultivate and co-opt criminal hackers," including Evil Corp.,[97] "enabling them to engage in disruptive ransomware attacks."[98]

In July 2021, the United States and a number of other countries accused China of "malicious cyber activity and irresponsible state behavior" for its use of criminal contract hackers to conduct unsanctioned cyber operations.[99] The United States claimed that Chinese government-affiliated "cyber-operators have conducted ransomware operations against private companies that have included ransom demands of millions of dollars," and attributed several attacks to hackers working with the Chinese Ministry of State Security.[100] U.S. officials condemned China's unwillingness to address criminal hacking activity by China-based groups.[101] On the same day, U.S. federal prosecutors announced indictment of four Chinese provincial

---

TION AND RELATED FREQUENTLY ASKED QUESTIONS; RUSSIA-RELATED DESIGNATIONS, (Apr. 15, 2021), https://home.treasury.gov/policy-issues/financial-sanctions/recent-actions/20210415 (listing 19 new individuals and 25 new entities).

96. *See* Press Release, U.S. Dep't of the Treasury, Treasury Sanctions Russia with Sweeping New Sanctions Authority (Apr. 15, 2021), https://home.treasury.gov/news/press-releases/jy0127 (stating that Russian Intelligence Services were responsible for the 2020 exploit of the SolarWinds Orion platform and other information technology infrastructures).

97. *See* discussion *infra* Section III.B.

98. *See* Press Release, U.S. Dep't of the Treasury, Treasury Sanctions Russia with Sweeping New Sanctions Authority (Apr. 15, 2021), https://home.treasury.gov/news/press-releases/jy0127.

99. *See* White House Statement, The United States, Joined by Allies and Partners, Attributes Malicious Cyber Activity and Irresponsible State Behavior to the People's Republic of China (July 19, 2021), https://www.whitehouse.gov/briefing-room/statements-releases/2021/07/19/the-united-states-joined-by-allies-and-partners-attributes-malicious-cyber-activity-and-irresponsible-state-behavior-to-the-peoples-republic-of-china/ (enumerating U.S. concerns with China's malicious cyber activity, including ransomware).

100. *Id.*

101. *See* Kochman & Stewart, *supra* note 15 (discussing indictments relating to China and Chinese hackers unsealed on July 19, 2021).

government intelligence officers for hacking dozens of U.S. computer systems.[102]

Ransomware hackers are believed to operate with impunity and even official encouragement in Iran as well. U.S. regulators have claimed that Iran has harbored the hackers responsible for a number of cyberattacks,[103] including the SamSam ransomware.[104] In September 2020, OFAC imposed sanctions on the Iranian intelligence ministry-backed cyber-attackers Advanced Persistent Threat 39 (APT39) and 45 associated persons for cyberattacks against perceived Iranian adversaries.[105]

3. *The Business of Ransoms and Ransomware-as-a-Service*

These days, ransomware extortion is a profitable industry. The Sodinokibi hackers are thought to have made over $81 million in 2020 alone.[106] Ransomware-as-a-Service (RaaS), in which software developers license their products to would-be hackers for a fixed fee or for a share of successful ransom pay-

---

102. Indictment, U.S. v. Ding Xiaoyang, No. 21 CR1622 GPC (S.D. Cal. May 28, 2021), https://www.law360.com/articles/1404209/attachments/0.

103. Zak Doffman, *Forget Russia—Iranian Hackers Behind Malicious New Cyber Attacks, Warns New Report*, FORBES (Nov. 12, 2020, 6:00 AM), https://www.forbes.com/sites/zakdoffman/2020/11/12/forget-russia-iranian-hackers-behind-malicuous-new-cyber-attacks-warns-new-report/?sh=65cf9357309a (quoting Lotem Finkelsteen that attacks being made on Israeli targets are further proof that the two countries express their aggression mostly through cyberattacks).

104. In December 2018, the U.S. Department of Justice indicted Faramarz Shahi Savandi and Mohammad Mehdi Shah Mansouri, both of Iran, for hacking and extortion. *See* Press Release, U.S. Dep't of Just., Two Iranian Men Indicted for Deploying Ransomware to Extort Hospitals, Municipalities, and Public Institutions, Causing Over $30 Million in Losses (Nov. 28, 2018), https://www.justice.gov/opa/pr/two-iranian-men-indicted-deploying-ransomware-extort-hospitals-municipalities-and-public (alleging both men acted from inside Iran). Additional charges were added a few weeks later. Kate Brumback, *2 Iranian Men Face New Charges Over Atlanta Cyberattack*, ASSOCIATED PRESS (Dec. 5, 2018), https://apnews.com/article/e81264497a074004a8bc042f4f05cdd1 (detailing additional charges).

105. *See* Press Release, U.S. Dep't of the Treasury, Treasury Sanctions Cyber Actors Backed by Iranian Intelligence Ministry (Sept. 17, 2020), https://home.treasury.gov/news/press-releases/sm1127 (accusing APT39 of deploying malware).

106. Ben Kochman, *IBM Says Ransomware Hackers Netted at Least $81M in 2020*, LAW360 (Sept. 28, 2020, 9:17 PM), https://www.law360.com/articles/1314366 (reporting on claims made by IBM's "X-Force" incident response unit).

ments,[107] has become common.[108] DarkSide, responsible for the Brenntag and Colonial Pipeline attacks discussed above, is an example of an RaaS operation.[109] In one model, the RaaS operator works with third-party hackers who gain access and encrypt the target devices. Another group, BlackMatter, posted advertisements on various cybercrime forums seeking partners, claiming its product combined the best features of REvil, Darkside and Lockbit, and touting added functions like printing the ransomware note on all available printers.[110] The RaaS team may then take 20–30% of the ransom payment, with the rest going to the hacker. Some developers create toolkits that can be downloaded and deployed by hackers with less technical skill;[111] others claim to enforce restrictions on potential targets.[112]

Ransomware victims even have their own version of customer service. Attackers have sharpened their business models, including guaranteeing turnaround times, providing real-

---

107. Edward Kost, *What Is Ransomware as a Service (RaaS)? The Dangerous Threat to World Security*, UpGuard: Blog (Aug. 24, 2021), https://www.upguard.com/blog/what-is-ransomware-as-a-service. This "as-a-service" model follows similar evolutions in the mainstream software and infrastructure industries, which have seen success from "software-as-a-service" and "infrastructure-as-a-service" business models. Ransomware Task Force, Inst. for Sec. & Tech., Combating Ransomware 16 (Apr. 30, 2021) https://securityandtechnology.org/wp-content/uploads/2021/04/IST-Ransomware-Task-Force-Report.pdf.

108. Marisa Midler, *Ransomware as a Service (RaaS) Threats*, Carnegie Mellon Univ.: Software Eng'g Inst. Blog (Oct. 5, 2020), https://insights.sei.cmu.edu/blog/ransomware-as-a-service-raas-threats/ (listing the top ten active ransomware variants in the first quarter of 2020 and noting that four of them use the RaaS model). The Sodinokibi/REvil, Phobos, Dharma, and GlobeImposter ransomware variants also all operate using an RaaS model. *Id.*

109. Abrams, *supra* note 70 (explaining that DarkSide partnered with third-party hackers who gained access to networks and encrypted devices).

110. Dmitry Smilyanets, *An Interview with BlackMatter: A New Ransomware Group That's Learning from the Mistakes of DarkSide and REvil,* The Record (Aug. 2, 2021), https://therecord.media/an-interview-with-blackmatter-a-new-ransomware-group-thats-learning-from-the-mistakes-of-darkside-and-revil/.

111. Juliana De Groot, *A History of Ransomware Attacks: The Biggest and Worst Ransomware Attacks of All Time*, Digital Guardian (Dec. 1, 2020), https://digitalguardian.com/blog/history-ransomware-attacks-biggest-and-worst-ransomware-attacks-all-time.

112. Smilyanets, *supra* note 110.

time chat support for victims, and offering payment demands customized to a victim's financial profile."[113] Some hackers have offered a help line for victims unsure how to buy bitcoin.[114] The ransomware group REvil reportedly set up custom-made sites for each of their victims to use to negotiate getting their data back, and advertised its successes (victims) on a publicly-available "happy blog."[115]

Frequently, the size of the ransom actually paid is negotiated. For example, the Washington, D.C., Metropolitan Police Department reportedly offered the Babuk ransomware group $100,000 in response to a $4 million demand in May 2021.[116] Babuk rejected the offer and claimed to have released 250GB of personal data of police personnel and informers.[117] Other negotiations have been more "successful." In January 2020, Travelex negotiated the ransom from $6 million down to $2.3 million.[118] When CWT Global suffered a Ragnar Locker ransomware attack in July 2020, the initial demand[119] was for $10 million. After discussions in an anonymous public chat room,

---

113. Stark, *supra* note 9.

114. Lawrence J. Trautman & Peter C. Ormerod, *Wannacry, Ransomware, and the Emerging Threat to Corporations*, 86 TENN. L. REV. 503, 535 (2019) (quoting Bruce Schneier, IBM Resilient Chief Technology Officer).

115. David E. Sanger, *Russia's Most Aggressive Ransomware Group Disappeared. It's Unclear Who Made That Happen.*, N.Y. TIMES (July 13, 2021, 10:32 AM), https://www.nytimes.com/2021/07/13/us/politics/russia-hacking-ransomware-revil.html?referringSource=articleShare.

116. *See* Thomas Brewster, *Ransomware Hackers Claim to Leak 250GB of Washington, D.C., Police Data After Cops Don't Pay $4 Million Ransom*, FORBES (May 13, 2021, 10:32 AM), https://www.forbes.com/sites/thomasbrewster/2021/05/13/ransomware-hackers-claim-to-leak-250gb-of-washington-dc-police-data-after-cops-dont-pay-4-million-ransom/?sh=51e794e558d0; Peter Hermann & Dalton Bennett, *Ransomware Attack on D.C. Police Resumes with More Internal Files Released*, WASH. POST (May 11, 2021, 6:58 PM), https://www.washingtonpost.com/local/public-safety/ransomware-attack-dc-police/2021/05/11/e1cb8600-b295-11eb-ab43-bebddc5a0f65_story.html (noting that the police stopped further theft of data but the hackers had already stolen a number of documents).

117. Brewster, *supra* note 116.

118. Akshaya Asokan, *Travelex Paid $2.3 Million to Ransomware Gang: Report*, BANK INFO SEC. (Apr. 10, 2020), https://www.bankinfosecurity.com/travelex-paid-23-million-to-ransomware-attackers-report-a-14094.

119. Jack Stubbs, *'Payment Sent' - Travel Giant CWT Pays $4.5 Million Ransom to Cyber Criminals*, REUTERS (July 31, 2020, 9:55 AM), https://www.reuters.com/article/us-cyber-cwt-ransom/payment-sent-travel-giant-cwt-pays-4-5-million-ransom-to-cyber-criminals-idUSKCN24W25W.

the hackers agreed to a bitcoin payment valued at $4.5 million.[120] As mentioned above, the Brenntag ransom of $4.4 million in Bitcoin paid in May 2021 had been reduced from the initial demand of approximately $7.5 million.[121]

D. *Ransomware Payment Mechanics*

1. *Cryptocurrencies*

Ransomware hackers typically demand that their victims send the ransom amount in a cryptocurrency,[122] such as Bitcoin,[123] capitalizing on the relatively unregulated ecosystem of the cryptocurrency markets.[124]

It is often said that cryptocurrencies are anonymous; it is more precise to say that they are generally held pseudonymously. A cryptocurrency is an entry on a digital ledger.[125] Ledger entries are signed, and only modifiable, by authorized parties.[126] The ledger itself, however, is distributed among users of the cryptocurrency, hence "distributed ledger."[127] Distribution of the ledger ensures accuracy; each transaction is

120. *Id.*

121. Abrams, *supra* note 70 (reporting the lower payment amount).

122. *See* Julio Hernandez-Castro, *An Economic Analysis of Ransomware and Its Welfare Consequences,* 7(3):190023 ROYAL SOCIETY OPEN SCIENCE 4 (Mar. 2020), https://www.researchgate.net/publication/339688144_An_economic_analysis_of_ransomware_and_its_welfare_consequences (noting that "Bitcoin and other cryptocurrencies have played a fundamental role in the 'success' of Cryptolocker and other recent ransomware").

123. *See* Custers et al., *supra* note 42 (noting that although Bitcoin is currently the most common, other cryptocurrencies such as Monero are gaining in popularity among ransomware hackers).

124. Cryptocurrencies add to the challenge of ransomware because they are considered to be borderless, and avoid compliance and other costs imposed by national financial regulation. RANSOMWARE TASK FORCE, INST. FOR SEC. & TECH., *supra* note 107, at 14 (calling cryptocurrencies "borderless").

125. *See* Nareg Essaghoolian, Comment, *Initial Coin Offerings: Emerging Technology's Fundraising Innovation*, 66 UCLA L. REV. 296, 302 (2019) (explaining briefly blockchain technology).

126. *See* Scott J. Shackelford & Steve Myers, *Block-by-Block: Leveraging the Power of Blockchain Technology to Build Trust and Promote Cyber Peace,* 19 YALE J.L. & TECH. 334, 345 (2017) (explaining the use of signing keys).

127. *See* Brandon Ferrick, Note, *Modernizing the Stockholder Shield: How Blockchains and Distributed Ledgers Could Rescue the Appraisal Remedy*, 60 B.C. L. REV. 621, 623 (2019) (describing distributed ledgers).

verified by other copies of the ledger.[128] As a result, each transaction is "named" and even public, not anonymous.[129]

The "names" on the ledger, however, are bitcoin addresses, represented by long alphanumeric strings that generally reveal little about the people involved.[130] Cryptocurrencies are transferred to and from, and held in, designated digital "wallets."[131] If a wallet is "hosted," a second party, like a cryptocurrency exchange, receives, stores, and transmits the currency on behalf of its accountholders.[132] An "unhosted" wallet is one not hosted by a third-party financial system, and has been analogized to an anonymous bank account.[133] If a wallet is unhosted, the beneficial owner of the wallet transfers money in and out of the wallet. Cryptocurrencies may also be moved around using smaller crypto kiosks and trading desks that may be difficult to track.[134]

---

128. *See* Bridget J. Crawford, *Blockchain Wills*, 95 IND. L.J. 735, 775 (2020) (explaining how blockchain verifies transactions by comparing it to a personal check).

129. *See* Nicole Perlroth et al., *Pipeline Investigation Upends Idea That Bitcoin is Untraceable,* N.Y. TIMES (June 9, 2021), https://www.nytimes.com/2021/06/09/technology/bitcoin-untraceable-pipeline-ransomware.html (explaining that all Bitcoin transactions are out in the open); Briseida Sofia Jiménez-Gómez, *Risks of Blockchain for Data Protection: A European Approach*, 36 SANTA CLARA HIGH TECH. L.J. 281, 293 (2020) (identifying most cryptocurrencies as pseudo-anonymous, not anonymous).

130. Aff. Supp. Appl. for Seizure Warrant, Case 3:21-mj-70945-LB (N.D. Cal. June 7, 2021), ¶ 18, https://www.justice.gov/opa/press-release/file/1402056/download (comparing bitcoin addresses with bank account numbers).

131. Bitcoin wallets allow users to send and receive bitcoins. They are software applications that interface with the Bitcoin blockchain and generate and store a user's address and private keys (passwords). *Id.* ¶¶ 19–20 (defining Bitcoin wallets and private keys).

132. *See* FIN. CRIMES ENF'T NETWORK, APPLICATION OF FINCEN'S REGULATIONS TO CERTAIN BUSINESS MODELS INVOLVING CONVERTIBLE VIRTUAL CURRENCIES, FIN-2019-G001 (May 9, 2019).

133. *See id.* (explaining some cryptocurrency basics in connection with the proposed rule regarding unhosted wallets).

134. Ben Kochman, *Ransomware Panel Urges Crypto Oversight, Payment Reports,* LAW360 (Apr. 29, 2021, 9:24 PM), https://www.law360.com/articles/1380203/ransomware-panel-urges-crypto-oversight-payment-reports (reporting on the Institute for Security and Technology Ransomware Task Force findings). *See also* RANSOMWARE TASK FORCE, INST. FOR SEC. & TECH., *supra* note 107, at 6 (prioritizing closer regulation of cryptocurrency exchanges, crypto desks, and over-the-counter trading desks, and recommending that

Much as a shell corporation may do business without needing to disclose the identity of the parties who ultimately benefit, cryptocurrency accounts are merely addresses with which values may be associated.[135] In addition, a ransom often does not flow straight from the ransomware victim to the hacker; it travels through a multi-step process involving different financial entities, many of which are still outside of established (regulated) financial payments markets.[136] Hackers may shuffle cryptocurrencies among various accounts to evade the few institutional safeguards operating in this space,[137] just as shell corporations may be used for money laundering, tax evasion, and the like. In sum, cryptocurrency transfers—including ransom payments—are generally difficult to connect with a particular person, which is why ransomware demands are usually for some quantity of a cryptocurrency.[138]

---

they be required to comply with laws relating to customer due diligence and anti-money laundering).

135. Carol Goforth, *The Lawyer's Cryptionary: A Resource for Talking to Clients about Crypto-Transactions*, 41 CAMPBELL L. REV. 47, 56 (2019) (defining cryptocurrency address).

136. RANSOMWARE TASK FORCE, INST. FOR SEC. & TECH., *supra* note 107 (describing steps in the process as "novel").

137. *See* U.S. DEP'T JUST., REPORT OF THE ATTORNEY GENERAL'S CYBER DIGITAL TASK FORCE 51 (2020), www.justice.gov/archives/ag/page/file/1326061/download (noting that many have sought to leverage new financial technology services as a way to "circumvent traditional financial institutions in order to obtain, transfer, and use funds to advance their missions"); *Terrorism Financing in Early Stages with Cryptocurrency But Advancing Quickly*, CHAINALYSIS: INSIGHTS (Jan. 17, 2020), https://blog.chainalysis.com/reports/terrorism-financing-cryptocurrency-2019 (expressing concern regarding advances in technical sophistication in terrorism financing); Yaya Fanusie, *The New Frontier in Terror Fundraising: Bitcoin*, CIPHER BRIEF (Aug. 24, 2016), https://www.thecipherbrief.com/column_article/the-new-frontier-in-terror-fundraising-bitcoin (discussing terrorist financial innovation); Resty Woro Yuniar, *Bitcoin, PayPal Used to Finance Terrorism, Indonesian Agency Says*, WALL ST. J. (Jan. 10, 2017, 10:46 AM), https://www.wsj.com/articles/bitcoin-paypal-used-to-finance-terrorism-indonesian-agency-says-1483964198 (reporting that virtual money was used to make tracking a transaction difficult for law enforcement).

138. RANSOMWARE TASK FORCE, INST. FOR SEC. & TECH., *supra* note 107 (noting that cryptocurrencies add to the challenge of identifying ransomware hackers).

That said, in some circumstances, blockchain explorers[139] and analysis can help interpret public ledgers and reveal individual identities.[140] However, even though law enforcement officials in the Colonial Pipeline and other cases have attributed identities to some digital currency addresses and recovered ransom amounts paid in a cryptocurrency,[141] the majority of transactions are still impossible to trace to a particular person.[142] Ransoms paid are, as a general matter, irrecoverable.

2. *Paying the Ransom*[143]

Recall our hospital victim from the introduction. The hospital promptly notifies its insurance provider, a digital forensics and incident response company, the Department of Health and Human Services,[144] and law enforcement. Soon, our hospital is told by the hackers to pay $10 million in bitcoin

---

139. A blockchain explorer is a software that draws data from a blockchain and uses a database to arrange and present the data to a user in a searchable format. Affidavit in Support of an Application for a Seizure Warrant at 5, No: 3:21-mj-70945-LB (N.D. Cal. June 7, 2021), https://www.justice.gov/opa/press-release/file/1402056/download (noting that blockchain explorers allow users to search for and review transactional data for addresses on a particular blockchain).

140. Blockchain analysis, often conducted by specialized blockchain analytic companies, can help interpret public blockchain ledgers and identify entities are involved in particular transactions. RANSOMWARE TASK FORCE, INST. FOR SEC. & TECH., *supra* note 107 (explaining blockchain analysis).

141. *See* discussion *infra* Sections III.B and V.F.

142. *See* Paul Vigna & Caitlin Ostroff, *Why Hackers Use Bitcoin and Why It Is So Difficult to Trace,* WALL ST. J. (July 16, 2020, 4:33 PM), https://www.wsj.com/articles/why-hackers-use-bitcoin-and-why-it-is-so-difficult-to-trace-11594931595 (explaining that no identifying information is needed to start a bitcoin account); Madana Prathap, *Bitcoin Does Not Make Payments Anonymous – Just Really Hard to Trace,* BUS. INSIDER INDIA (Aug. 5, 2021), https://www.businessinsider.in/investment/news/bitcoin-does-not-make-payments-anonymous-just-really-hard-to-trace/articleshow/85068905.cms (discussing recent improvements in efforts to link wallet addresses to persons); Requirements for Certain Transactions Involving Convertible Virtual Currency or Digital Assets, 85 Fed. Reg. 83.840, 83,844 (proposed Dec. 23, 2020) (to be codified at 31 C.F.R. Parts 1010, 1020, 1022) (outlining limitations of current tools to identify attribute some activity in convertible virtual currencies to natural persons).

143. *See generally* RANSOMWARE TASK FORCE, INST. FOR SECURITY. & TECH., *supra* note 107, at Appendix B (walking through the steps of the cryptocurrency payment process).

144. 45 C.F.R. § 164.304 (2021) (defining "security incident").

to an address provided. The hospital is scrambling—its care providers are struggling with paper charting and the information in its offsite back-up system is being scanned to make sure it is even usable. Confronted with the specter of compromised patient care, the hospital decides to pay the ransom. How is this payment made?

In a typical arrangement,[145] the hospital might send $10 million by wire transfer from its bank to a cryptocurrency exchange like Coinbase,[146] with instructions to purchase the equivalent amount in bitcoin. The actual transfer of funds may be effected by the hospital itself, or by the incident response team, or even by the hospital's insurer. The bitcoin is then sent from a wallet hosted at the exchange to an address designated by the hacker.

At that point, a hacker typically begins splitting up the funds and moving them around in order to conceal the identity of the ultimate beneficiaries.[147] Sometimes the funds are spread out among hundreds of other wallets.[148] This process may include the following colorfully named, and somewhat overlapping, operations:

- mixers and tumblers,[149] muddying the public ledger by mixing in legitimate traffic with illicit ransomware funds;[150]
- smurfing[151] transactions, breaking the total amount into many smaller amounts across many accounts and exchanges;

---

145. FIN. CRIMES ENF'T NETWORK, ADVISORY ON RANSOMWARE AND THE USE OF THE FINANCIAL SYSTEM TO FACILITATE RANSOM PAYMENTS 3 (2021), https://www.fincen.gov/sites/default/files/advisory/2021-11-08/FinCEN%20Ransomware%20Advisory_FINAL_508_.pdf (outlining a typical fact pattern).

146. COINBASE, https://www.coinbase.com (last visited Jul. 24, 2021).

147. *See* Custers et al., *supra* note 42.

148. David Uberti, *How the FBI Got Colonial Pipeline's Ransom Money Back*, WALL ST. J. (June 11, 2021, 5:33 AM), https://www.wsj.com/articles/how-the-fbi-got-colonial-pipelines-ransom-money-back-11623403981 (explaining how the payment was tracked).

149. Mixing or tumbling involves the use of mechanisms to break the connection between an address sending cryptocurrency and the addresses receiving cryptocurrency. FIN. CRIMES ENF'T NETWORK, *supra* note 145 (defining some common terms).

150. RANSOMWARE TASK FORCE, INST. FOR SEC. & TECH., *supra* note 107, at 14 (explaining how funds are mixed with legitimate traffic).

151. Smurfing refers to a layering technique in money laundering that involves breaking total amounts of funds into smaller amounts to move

- "chainhopping," exchanging funds in one cryptocurrency for another using any of a variety of cryptocurrency exchanges;[152]
- money-mules, using service providers to set up accounts, or using accounts with false or stolen credentials;[153] and
- simply moving the cryptocurrency to exchanges and peer-to-peer exchangers[154] in jurisdictions with weak anti-money laundering and anti-terrorism financing controls.

If all goes well, when the hospital pays the ransom, the hospital begins to regain control over its data. The regained control, however, is necessarily partial. It will be unclear whether patient data was exfiltrated and, if so, whether there remains a risk that the data will be released on the web. The digital forensics and incident response team begins the process of tracing the ransomware to identify how it was installed,[155] and to the extent possible, to determine whether the malware is still in the hospital system as a back door for another attack. It will be difficult, maybe impossible, for the hospital to be positive that remediation is complete and risks have been contained.

The incident is likely to be costly. The hospital may need to overhaul or even replace its entire computer system. Patients whose care may have been compromised during the outage may sue.[156] It may be unclear what costs the hospital's

---

through multiple accounts before they reach the ultimate beneficiary. FIN. CRIMES ENF'T NETWORK, *supra* note 145 (defining some common terms).

152. RANSOMWARE TASK FORCE, INST. FOR SEC. & TECH., *supra* note 107, at 14 (defining chainhopping).

153. *Id.* (noting illicit account use). *See* Custers et al., *supra* note 42.

154. Peer-to-peer exchangers operate informally, exchanging fiat currencies for virtual currencies or one virtual currency for another virtual currency. *See* FIN. CRIMES ENF'T NETWORK, ADVISORY ON ILLICIT ACTIVITY INVOLVING CONVERTIBLE VIRTUAL CURRENCY 4 (2019), https://www.fincen.gov/sites/default/files/advisory/2019-05-10/FinCEN%20Advisory%20CVC%20FINAL%20508.pdf.

155. It is often a condition to ransomware negotiations that the hacker disclose how it gained access to the victim's network. *See* Abrams, *supra* note 70 (discussing the Brenntag ransomware).

156. For example, four class action suits (two in federal court, two in California state court) were filed against Scripps Healthcare alleging negligent behavior by the hospital. Heather Landi, *Scripps Health Was Attacked by Hackers. Now, Patients Are Suing for Failing to Protect Their Health Data,* FIERCE

cyber insurance policy will cover. Concerned with disclosure of patients' protected health information in violation of the Health Insurance Portability and Accountability Act of 1996 (HIPAA),[157] the Department of Health and Human Services' Office of Civil Rights may penalize the hospital.[158] If our hypothetical hospital is for-profit, given a likely drop in share value, its shareholders may sue.[159] The hospital's woes may continue

---

HEALTHCARE (June 22, 2021, 3:45 PM), https://www.fiercehealthcare.com/tech/following-ransomware-attack-scripps-health-now-facing-class-action-lawsuits-over-data-breach#:~:text=corning's%20lawsuit%20wants%20Scripps%20Health,litigation%20expenses%20and%20court%20costs (discussing the Scripps lawsuits); Shawn Rice, *Cyberattack Class Suits Have Unpredictable Insurance Impact,* LAW360 (June 30, 2020), https://www.law360.com/articles/1399182/cyberattack-class-suits-have-unpredictable-insurance-impact (discussing costs companies face after a cyberattack).

157. Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (1996) (codified as amended in scattered sections of 5–42 U.S.C.).

158. Ransomware is a security incident under the HIPAA Security Rule and there is liability for not reporting it. A security incident is defined as the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system. 45 C.F.R. § 164.304 (2013). Once the ransomware is detected, the covered entity or business associate must initiate security incident and response and reporting procedures. 45 C.F.R. § 164.308(a)(6) (2013). In addition, a ransomware attack may result in an impermissible disclosure of patient protected health information and breach HIPAA rules. *See* 45 C.F.R. § 160.103 (2013) (defining disclosure); 45 C.F.R. § 164.402 (2013) (defining breach as the acquisition, access, use, or disclosure of patient protected health information which compromises the security or privacy of the information).

See also U.S. DEP'T HEALTH & HUMAN SERVS., FACT SHEET: RANSOMWARE AND HIPAA (2016), https://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf ("When electronic protected health information (ePHI) is encrypted as the result of a ransomware attack, a breach has occurred because the ePHI encrypted by the ransomware was acquired (i.e., unauthorized individuals have taken possession or control of the information), and thus is a "disclosure" not permitted under the HIPAA Privacy Rule."). HIPAA violations by covered entities may be intentional or unintentional, although a breach as a result of a malicious cyberattack might qualify as a Tier 1 violation (a violation that the covered entity was unaware of and could not have realistically avoided, had a reasonable amount of care been taken to abide by HIPAA rules). *What Are the Penalties for HIPAA Violations,* HIPAA JOURNAL (Jan. 15, 2021), https://www.hipaajournal.com/what-are-the-penalties-for-hipaa-violations-7096/ (walking through the four tiers).

159. This assumes a for-profit hospital.

long after the hackers have sent the key and the computer system is again operational.

To make matters even worse, however, the Department of the Treasury may take enforcement actions against the hospital, its incident response company, its insurance company, and its bank based on the payment made to the hackers. As discussed below, if regulators determine that the hackers are sanctioned persons, or that the transfer violated anti-money laundering laws, then the government may prosecute the hospital and those who assisted it.

II.
National Security and Liability for Paying Ransoms

A. *National Security and the Flow of Value*

Ransomware is a national security issue; it is not merely "private" criminal extortion,[160] and it poses a threat to U.S. critical infrastructure[161] including military facilities. In July 2019, the U.S. Coast Guard issued a marine safety alert[162] after a ransomware attack on a U.S.-flagged ultra-large container ship highlighted dangers to vessel and facility owners and operators.[163] In December 2019, the Coast Guard announced

---

160. Ransomware Task Force, Inst. for Sec. & Tech., *supra* note 107, at 7 (explaining that cybercrime is typically seen as white-collar crime, but ransomware presents a national security threat). *See also* Jeff Neal, *Is the U.S. in a Cyber War?*, Harv. L. Today (July 14, 2021), https://today.law.harvard.edu/is-the-u-s-in-a-cyber-war/?utm_source+SilverpopMailing&utm_medium=email&utm_campaign=daily%20Gazette%2020210719%20(1) (interviewing Juliette Kayyem, who notes that U.S. public infrastructure is owned by the private sector, and that cyberattacks against private entities may impact public sector downstream clients).

161. *See* Cybersecurity & Infrastructure Sec. Agency, Critical Infrastructure Sectors, https://www.cisa.gov/critical-infrastructure-sectors (last visited July 30, 2021) (listing 16 sectors).

162. U.S. Coast Guard, Cyber Incident Exposes Potential Vulnerabilities Onboard Commercial Vessels, (July 8, 2019), https://www.dco.uscg.mil/Portals/9/DCO%20Documents/5p/CG-5PC/INV/Alerts/0619.pdf (claiming the vessel was operating without effective cybersecurity measures).

163. James Rundle, *Coast Guard Details February Cyberattack on Ship,* Wall St. J. (July 26, 2019), https://www.wsj.com/articles/coast-guard-details-february-cyberattack-on-ship-11564133401 (reporting an Emotet malware infection that debilitated a deep-draft vessel, bound for New York City); *Ryuk Ransomware Took Down U.S. Coast Guard Operations,* CISOMAG (Dec. 3, 2019), https://cisomag.eccouncil.org/ryuk-ransomware-took-down-u-s-coast-guard-

that a ransomware attack had penetrated a U.S. port, and encrypted critical network files, including those that monitored and controlled cargo transfer.[164] The facility was shut down for over 30 hours.[165] Experts warn that "attacks on the energy grid, on a nuclear plant, waste treatment facilities, or on any number of critical assets could have devastating consequences, including human casualties."[166]

Ransomware also poses risks to the healthcare system. Healthcare facilities have been a favorite target of ransomware hackers with 560 U.S. healthcare facilities victimized in 2020.[167] An October 2020 ransomware attack on the University of Vermont Health Network reportedly delayed cancer treatments for some patients.[168]

Educational institutions and local governments have also been disrupted, and their funding (often taxpayer dollars) diverted.[169] Almost 1,700 schools, colleges, and universities in the United States were impacted by ransomware in 2020.[170] Many of those educational institutions were already struggling with budgetary issues and COVID-19-related challenges. When the county school district in Yazoo, Mississippi, voted to pay a

---

operations/ (identifying the attack as deploying Ryuk ransomware); Cybereason Nocturnus, *A One-Two Punch of Emotet, TrickBot & Ryuk Stealing and Ransoming Data*, MALICIOUS LIFE (Apr. 2, 2019), https://www.cybereason.com/blog/one-two-punch-emotet-trickbot-and-ryuk-steal-then-ransom-data (explaining that a number of attacks adapted Emotet as a dropper for the TrickBot trojan, which then stole sensitive information and downloaded the Ryuk ransomware).

164. COMMANDANT, U.S. COAST GUARD, MARINE SAFETY INFO. BULLETIN: CYBERATTACK IMPACTS MTSA FACILITY OPERATIONS (Dec. 16, 2019), https://www.dco.uscg.mil/Portals/9/DCO%20Documents/5p/MSIB/2019/MSIB_10_19.pdf (announcing a Ryuk ransomware attack).

165. *See id.*; CISOMAG, *supra* note 163.

166. RANSOMWARE TASK FORCE, INST. FOR SEC. & TECH., *supra* note 107, at 8 (detailing incidents in which ransomware has disrupted U.S. critical infrastructure).

167. *The State of Ransomware in the US: Report and Statistics 2020,* EMSISOFT MALWARE LAB (Jan. 18, 2021), https://blog.emsisoft.com/en/37314/the-state-of-ransomware-in-the-us-report-and-statistics-2020/.

168. Lindsey O'Donnell, *Cyberattack on UVM Health Network Impedes Chemotherapy Appointments*, THREATPOST (Nov. 9, 2020, 3:15 PM), https://threatpost.com/cyberattack-uvm-health-network/161059/ (reporting that the attack halted chemotherapy, mammogram, and biopsy appointments).

169. RANSOMWARE TASK FORCE, INST. FOR SEC. & TECH., *supra* note 107, at 9.

170. *The State of Ransomware in the US, supra* note 167.

cybersecurity firm to help recover maliciously encrypted data, it used up a chunk of its annual budget.[171] An attack on a Houston-area school district in 2020 jeopardized its ability to function and to make payroll.[172] Local governments, which oversee water utilities, airports, schools, health care facilities, and other services, are also frequent targets.[173] Victims have included the City of Atlanta,[174] the City of Baltimore,[175] and the Colorado Department of Transportation.[176] Such attacks have been described as "catastrophic" for both the governments and their constituents.[177]

The economic impact of ransomware attacks is substantial and, as suggested in the foregoing section, far greater than the value of the ransoms actually paid.[178] A ransomware attack may force a victim offline for weeks,[179] followed by a recovery

---

171. RANSOMWARE TASK FORCE, INST. FOR SEC. & TECH., *supra* note 107, at 10.

172. McMillan, *supra* note 50 (enumerating a number of attacks).

173. Michael Garcia, *The Underbelly of Ransomware Attacks: Local Governments,* COUNCIL ON FOREIGN RELATIONS BLOG (May 10, 2021, 12:35 PM), https://www.cfr.org/blog/underbelly-ransomware-attacks-local-governments (noting local governments "are one of the most targeted sectors, yet have arguably the least resources and capabilities to prepare for and respond to ransomware").

174. Alan Blinder & Nicole Perlroth, *A Cyberattack Hobbles Atlanta, and Security Experts Shudder,* N.Y. TIMES (Mar. 27, 2018), https://www.nytimes.com/2018/03/27/us/cyberattack-atlanta-ransomware.html (detailing the attack).

175. Niraj Chokshi, *Hackers Are Holding Baltimore Hostage: How They Struck and What's Next,* N.Y. TIMES (May 22, 2019), https://www.nytimes.com/2019/05/22/us/baltimore-ransomware.html (noting that Baltimore responded quickly but was still impacted).

176. Tamara Chuang, *Cyber Attack on CDOT Computers Estimated to Cost Up to $1.5 Million So Far,* DENVER POST (Apr. 6, 2018, 12:11 AM), https://www.denverpost.com/2018/04/05/samsam-ransomware-cdot-cost/ (noting the costs of the attack).

177. RANSOMWARE TASK FORCE, INST. FOR SEC. & TECH., *supra* note 107, at 35 (recommending a requirement that local governments adopt baseline security measures).

178. *See* Jacob Bunge & Jesse Newman, *Ransomware Attack Roiled Meat Giant JBS, Then Spilled Over to Farmers and Restaurants,* WALL ST. J. (June 11, 2021, 10:28 AM) (noting JBS paid an $11 million ransom, but in 2020 generated $53 billion in global sales).

179. *Ransomware Payments Fall as Fewer Companies Pay Data Exfiltration Extortion Demands,* COVEWARE (Feb. 1, 2021), https://www.coveware.com/blog/ransomware-marketplace-report-q4-2020. Cybersecurity experts estimate that it takes organizations infected with ransomware on average over 16 days to restore their networks. Danny Palmer, *Ransomware Attacks are Causing More*

process that may take the better part of a year.[180] Total remediation costs are typically several times the ransom payment and are often large enough to cripple small businesses.[181] The National Cyber Security Alliance estimates that 60% of small businesses fail within six months of a cyberattack.[182] The global cost in 2020 was estimated at $20 billion.[183]

Apart from direct damages to the victims of ransomware attacks, the proceeds from such attacks are by definition funneled to criminal networks. One U.S. Department of Justice (DOJ) official called ransomware a "cyber weapon of mass destruction," operating in an unvirtuous cycle in which ransoms that are paid are used to develop more ransomware.[184] Proceeds may help finance terrorism, human trafficking, or the proliferation of weapons of mass destruction,[185] i.e., threaten security, and thereby impose further material and human costs. To simplify, payment to the wrong actor is itself a threat. The United States protects national security and public order by regulating money flows; OFAC sanctions, anti-money laundering regulations, and anti-terrorism acts, to name a few, all recognize that national security is protected by stopping the flow of funds to hostile actors.

Regulators can and do seek the potential attackers—the recipients of funds—directly. They may also try to stem the flow of funds at their sources. Usually, we associate those efforts with persons who are knowingly funding the potential attackers, but that is not necessarily the case. It is possible to use

---

Downtime Than Ever Before, ZDNET (Jan. 23, 2020), https://www.zdnet.com/article/ransomware-attacks-are-causing-more-downtime-than-ever-before/.

180. *The State of Ransomware in the US*, *supra* note 167.

181. RANSOMWARE TASK FORCE, INST. FOR SEC. & TECH., *supra* note 107, at 10.

182. Thomas Koulopoulos, *60 Percent of Companies Fail in 6 Months Because of This (It's Not What You Think)*, INC.COM (May 11, 2017), https://www.inc.com/thomas-koulopoulos/the-biggest-risk-to-your-business-cant-be-eliminated-heres-how-you-can-survive-i.html (noting almost 50% of small businesses have experienced a cyberattack).

183. *See* N.Y. DEP'T FIN. SERVS., INS. CIRCULAR LETTER NO. 2, INDUS. GUIDANCE REGARDING CYBER INS. RISK FRAMEWORK, 23 NYCRR 500 (July 1, 2021), https://www.dfs.ny.gov/industry_guidance/circular_letters/cl2021_02 (outlining ransomware risks to insurers).

184. McMillan, *supra* note 50 (quoting John Carlin of the DOJ). *See also id.*

185. RANSOMWARE TASK FORCE, INST. FOR SEC. & TECH., *supra* note 107, at 3 (warning that ransom money may go on to fund other types of crime).

existing legal tools to penalize persons who are providing the funds either unknowingly or under duress, such as ransomware victims. In these cases, the government may determine that its interest in interdicting the hostile actor outweighs the additional harm that may be imposed on the ransomware victim. When this occurs, regulators such as OFAC or FinCEN may punish ransomware victims who pay the ransom and those who assist them.

B. *OFAC Sanctions Liability*

1. *U.S. Sanctions in General*

OFAC administers a variety of measures restricting interaction between U.S. persons and persons the United States has determined to be a threat to our national security. Under the Trading with the Enemy Act[186] and, since the mid-1970s,[187] the National Emergencies Act[188] and the International Emergency Economic Powers Act,[189] the President has the authority to declare an emergency or national security threat, and to delegate authority for additional measures to the Treasury Department.

The result is a regulatory structure that currently includes restrictions relating to approximately 25 countries.[190] For example, U.S. persons are prohibited from dealing with ransomware attackers located in or affiliated with the govern-

186. 50 U.S.C. § 4305(b)(1)(B) (2018) (authorizing the President of the United States "during the time of war" to prevent or prohibit transactions in any property in which a foreign country or national has any interest by any person subject to the jurisdiction of the United States).

187. CHRISTOPHER A. CASEY ET AL., CONG. RSCH. SERV., R45618, THE INTERNATIONAL EMERGENCY ECONOMIC POWERS ACT: ORIGINS, EVOLUTION, AND USE, 8-10 (2020) (chronicling the transition from the Trading with the Enemy Act to the National Emergencies Act and the International Emergency Economic Powers Act).

188. 50 U.S.C. § 1601 *et seq.* (2018) (providing the requirements for the President to declare a national emergency).

189. 50 U.S.C. §§ 1701–07 (2018) (empowering the President to investigate, regulate, and prohibit certain transactions in the event of any unusual and extraordinary threat to national security from outside the country).

190. *Sanctions Programs and Country Information,* OFAC, U.S. DEP'T TREAS., https://home.treasury.gov/policy-issues/financial-sanctions/sanctions-programs-and-country-information (last visited July 30, 2021) (listing the active sanctions programs). Sanctions include bans on certain interactions unless the person gets a license from OFAC, and such licenses are difficult to get.

ments of jurisdictions such as Iran, North Korea, Syria, Cuba, Venezuela, and the Crimea region of Ukraine.[191] In addition, OFAC imposes measures on a variety of nonstate actors and behaviors through other programs, including its Counter Terrorism Sanctions[192] and Cyber-Related Sanctions.[193] Those restrictions may include a ban on certain transactions and asset freezes.[194] In connection with its sanctions programs, OFAC maintains a list of approximately 6,300 SDNs.[195] All U.S. persons are prohibited from dealing with SDNs, and any SDN property or interest in property within the possession or control of a U.S. person must be frozen and promptly reported to OFAC.[196] Entities owned 50% or more by SDNs trigger the

191. *Id.* (listing all U.S. sanctions programs, including the ones mentioned). *See also* OFAC, U.S. DEP'T TREAS., UPDATED ADVISORY ON POTENTIAL SANCTIONS RISKS FOR FACILITATING RANSOMWARE PAYMENTS, *supra* note 26, at 3–4 (describing those areas as subject to "comprehensive" embargoes).

192. *Counter Terrorism Sanctions*, OFAC, U.S. DEP'T TREAS., https://home.treasury.gov/policy-issues/financial-sanctions/sanctions-programs-and-country-information/counter-terrorism-sanctions (providing information about the counter-terrorism sanctions administered by OFAC) (last visited July 30, 2021).

193. *Sanctions Related to Significant Malicious Cyber-Enabled Activities*, OFAC, U.S. DEP'T TREAS., https://home.treasury.gov/policy-issues/financial-sanctions/sanctions-programs-and-country-information/sanctions-related-to-significant-malicious-cyber-enabled-activities (providing information about the cyber-related sanctions administered by OFAC) (last visited July 30, 2021). *See* Exec. Order No. 13,694, 80 Fed. Reg. 18077 (Apr. 2, 2015) (blocking the property of certain persons engaging in significant malicious cyber-enabled activities). Other sanctions programs under, for example, the Countering America's Adversaries Through Sanctions Act of 2017 may also be relevant in the ransomware context. *See, e.g.*, Countering America's Adversaries Through Sanctions Act, 22 U.S.C. §§ 9501–64 (2021), specifically § 9524 (relating to the imposition of sanctions with respect to activities of the Russian Federation undermining cybersecurity).

194. Sanctions programs vary, but for a general summary of the kinds of measures they include, see *Frequently Asked Questions*, OFAC, U.S. DEP'T TREAS., https://home.treasury.gov/policy-issues/financial-sanctions/faqs/topic/1501 (last visited July 29, 2021) (summarizing prohibited transactions and asset freezes).

195. *Where is OFAC's Country List? What Countries Do I Need to Worry About in Terms of U.S. Sanctions?*, OFAC, U.S. DEP'T TREAS., https://home.treasury.gov/policy-issues/financial-sanctions/sanctions-programs-and-country-information/where-is-ofacs-country-list-what-countries-do-i-need-to-worry-about-in-terms-of-us-sanctions (last visited July 29, 2021) (providing a good introduction to sanctions programs).

196. *See* Krauland et al., *supra* note 28.

same restrictions and requirements.[197] OFAC regulatory compliance measures, often transaction monitoring software, are a part of normal operations at entities such as financial institutions.[198]

2. *Who Has to Comply with OFAC Regulations?*

OFAC restrictions are primarily directed toward U.S. persons,[199] who are prohibited from making ransomware payments in violation of its regulations. U.S. persons include U.S. citizens and permanent residents, entities organized under U.S. laws, and any persons in the United States.[200]

OFAC's jurisdiction is broad, however. Some non-U.S. persons, whether ransomware victims or those who assist with the ransom payment, may also have to comply with OFAC regulations when their activities have a sufficient U.S. nexus. "Non-U.S. companies are subject to U.S. jurisdiction to the extent that they act within the United States, which includes acting through U.S.-incorporated entities or engaging in transactions involving U.S. goods, persons, or entities."[201] Non-U.S.

197. *Id.*

198. STEPHEN MARK LEVY, FEDERAL MONEY LAUNDERING REGULATION: BANKING, CORPORATE AND SECURITIES COMPLIANCE § 10.10 (2021, 2d ed. Supp. 2021-2) https://1.next.westlaw.com/Document/Iaa92444cb93911de9b8c850332338889/View/FullText.html?originationContext=typeAhead&transitionType=default&contextData=(sc.Default) (outlining OFAC sanctions compliance programs in the financial institutions context).

199. Most OFAC programs apply to "U.S. persons." Some OFAC sanctions relating to Cuba and North Korea, promulgated pursuant to the Trading with the Enemy Act, apply to a potentially broader category of "persons subject to the jurisdiction of the United States." *See* Amy Deen Westbrook, *What's in Your Portfolio? U.S. Investors Are Unknowingly Financing State Sponsors of Terrorism,* 59 DEPAUL L. REV. 1151, 1163 & n.65 (2010) (explaining the difference in jurisdiction between programs promulgated pursuant to the Trading with the Enemy Act and ones that have been imposed using the International Emergency Economic Powers Act).

200. 31 C.F.R. § 560.314 (defining the term "U.S. person" in the context of the Iranian Transactions and Sanctions Regulations).

201. Alexis Collins et al., *Ransomware and Sanctions Compliance: Considerations for Responses to Attacks,* CLEARY CYBERSECURITY & PRIVACY WATCH (Sept. 14, 2020) https://www.clearycyberwatch.com/2020/09/ransomware-and-sanctions-compliance-considerations-for-responses-to-attacks/ (warning "U.S. authorities view their jurisdiction expansively"). So, for example, a "non-U.S. company seeking to make a ransom payment to a sanctioned entity would thus be prohibited from making U.S. dollar transactions (almost all of which are routed and cleared through the U.S. financial system) for

persons may also be at risk for dealings with SDNs and comprehensively sanctioned jurisdictions under OFAC's "secondary sanctions" regimes. Secondary sanctions target non-U.S. persons who deal with SDNs, who participate in specified industries in sanctioned countries, or who support certain end-uses of concern[202] such as malicious cyber-activities outside U.S. jurisdiction.[203]

Thus, to the extent that a ransom is paid to an SDN (and so prohibited), the ransomware victim as well as those who assist the victim risk running afoul of the OFAC sanctions. Some at OFAC have suggested that sanctions enforcement in the wake of a ransomware payment may also be directed towards the attorneys involved in the ransomware response (in fact, there is some question of whether attorneys may be held to an even higher standard).[204]

3. *OFAC Advisory: Ransomware-Related Sanctions Targets*

In 2020 and 2021, OFAC issued and updated an advisory (the OFAC Advisory) warning that the agency adopts a strict liability approach to payments that make their way to an SDN, an entity over 50% owned by an SDN, or a threat actor in a sanctioned jurisdiction.[205] This approach will apply even if the ransomware victim makes the payment with no idea as to the

---

the purchase of digital currencies used for a ransom payment, or engaging with U.S. persons or entities, including U.S.-based digital currency exchanges and intermediaries, in facilitating such payment." *Id.*

202. *See* Krauland et al., *supra* note 28.

203. The jurisdiction of Executive Order No. 13,694 is broad. *See* Exec. Order 13,694, § 1(a)(ii)(B), 80 Fed. Reg. 18077 (Apr. 2, 2015) (authorizing sanctions against non-U.S. persons who materially assist or provide financial support for any persons blocked under the order). In addition, Executive Order No. 13722 authorizes secondary sanctions against persons who materially assist or provide financial support for persons sanctioned for engaging in malicious cyber activities. *See* Exec. Order 13,722, § 2(a)(vii), 81 Fed. Reg. 14943 (Mar. 18, 2016) (imposing certain restrictions on North Korea). Arguably, any non-U.S. person, regardless of location, risks being designated on the SDN List for making a payment in any currency to a person sanctioned under the 2015 executive order. Collins et al., *supra* note 201.

204. *See* Stark, *supra* note 7 (discussing comments made at a January 2021 conference by Kaveh Miremadi, section chief in OFAC's enforcement division).

205. Off. of Foreign Assets Control, U.S. Dep't of the Treasury, *supra* note 26 (updating its October 1, 2020, advisory warning of potential sanctions for paying ransoms).

hacker's identity, and if the hacker's identity is not discovered until after the fact.

The SDN list currently includes ransomware hackers or identified ransomware attackers designated through, for example, the terrorism and cyber-related programs[206] as well as hackers connected with sanctioned jurisdictions.[207] As mentioned above, "U.S. law generally prohibits facilitating, enabling, tendering, etc. payment to a suspected terrorist or someone located in, or affiliated with, a jurisdiction subject to comprehensive U.S. sanctions—such as Iran and North Korea."[208] In addition, some SDNs are now identified as cryptocurrency wallet addresses.[209]

A ransomware attacker may be on the SDN list, or in a sanctioned jurisdiction, but, in many cases, the ransomware victim does not know.[210] Ransomware attackers typically employ their technology to conceal their identity and location. In addition, some hackers identified by OFAC are rebranding their ransomware or impersonating other groups in order to circumvent U.S. sanctions.[211] For example, EvilCorp has reportedly rebranded WastedLocker as "Hades," "Phoenix," and

---

206. Collins et al., *supra* note 201 (walking through the 2015 and 2016 Executive Orders pursuant to which cybersecurity threats may be sanctioned).

207. *Id.* (explaining prohibitions on ransom payments to persons located, organized, or resident in sanctioned territories).

208. Stark, *supra* note 7.

209. On November 28, 2018, OFAC identified for the first time digital currency addresses associated with sanctioned persons when it sanctioned two Iranian individuals involved in the 2015 SamSam ransomware scheme. Paul Marquardt et al., *OFAC Lists Digital Currency Addresses for First Time, Releases New Guidance,* CLEARY INT'L TRADE & SANCTIONS WATCH (Dec. 5, 2018) https://www.clearytradewatch.com/2018/12/ofac-lists-digital-currency-addresses-first-time-releases-new-guidance/ (noting that the individuals were accused of converting digital currency payments into Iranian rial as part of a widespread ransomware scheme).

210. Phil Muncaster, *Evil Corp Rebrands Ransomware to Escape Sanctions*, INFOSECURITY MAGAZINE (June 8, 2021) https://www.infosecurity-magazine.com/news/evil-corp-rebrands-ransomware/ (reporting that EvilCorp malware is identifiable based on things like the obfuscator, the cryptographic scheme, the encrypted file format, and other factors).

211. Elizabeth Montalbano, *Evil Corp Impersonates PayloadBin Group to Avoid Federal Sanctions*, THREATPOST (June 8, 2021) https://threatpost.com/evil-corp-impersonates-payloadbin/166710/ (reporting that Evil Corp. was trying to mask its latest activity by using a previously unknown ransomware called PayloadBin).

most recently "PayloadBin" (on a site previously operated by the Babuk group, which carried out the cyberattack on the DC police[212]) in "an attempt to trick victims into violating the OFAC regulations."[213] Even if a victim has some idea of who originated the attack, proving definitively that a hacker is *not* on the SDN list is difficult.[214]

4. *Strict Liability, Licenses, and Penalties*

Because U.S. sanctions regimes may impose strict liability in civil cases, an entity that makes a ransom payment to a hacker sanctioned by the United States could be subject to severe monetary penalties regardless of whether the entity knew or had reason to know that the hacker was sanctioned.[215] The OFAC Advisory warned of civil penalties for sanctions violations[216] based on strict liability, and emphasized that "a person subject to U.S. jurisdiction may be held civilly liable even if such person did not know or have reason to know that it was engaging in a transaction that was prohibited under sanctions laws and regulations administered by OFAC."[217]

OFAC has wide discretion to begin an investigation, and, although the agency will likely consider the company's knowledge when determining whether to bring an enforcement action, the action itself may impose significant costs on a ran-

212. *See* discussion *supra* Section II.C.3.

213. Muncaster, *supra* note 210 (noting the effort to trick victims).

214. *See* Stark, *supra* note 7. *See also* Krauland et al., *supra* note 28 (noting that ransomware victims and those who assist them are often incapable of determining the identity or the location of a ransomware hacker).

215. *See* Alexis Collins et al., *OFAC and FinCEN Issue Advisories on Cyber Ransom Payments,* Cleary Cybersecurity & Privacy Watch, Cleary Gottlieb (Oct. 6, 2020), https://www.clearycyberwatch.com/2020/10/ofac-and-fincen-issue-advisories-on-cyber-ransom-payments/ (noting OFAC's strict liability approach). *See also* Krauland et al., *supra* note 28.

216. Off. of Foreign Assets Control, U.S. Dep't of the Treasury, *supra* note 26, at 4 (updating the October 1, 2020, advisory). Violation of U.S. sanctions, prohibited interactions without an OFAC license, may result in monetary penalties, and willful violations may trigger DOJ criminal prosecution. Roberto J. Gonzalez & Rachel M. Fiorill, *USA*, *in* Sanctions 2020 151, 151 (2019), https://www.paulweiss.com/media/3979073/iclg_sanctions2020.pdf.

217. Off. of Foreign Assets Control, U.S. Dep't of the Treasury, *supra* note 26, at 4 (updating the October 1, 2020, advisory to encourage victims to report attacks if they suspect—not just believe there to be—a sanctions nexus).

somware target.[218] The OFAC Advisory mentioned potential mitigating factors that OFAC will consider, including timely and complete reporting of a ransomware attack,[219] cooperation with law enforcement, and cyber-security compliance measures.[220] But the availability of mitigation credit is unclear when a sanctions nexus is known or suspected at the time of the attack.[221]

The OFAC Advisory further warned companies that "license applications involving ransomware payments demanded as a result of malicious cyber-enabled activities will continue be reviewed by OFAC on a case-by-case basis with a presumption of denial."[222] OFAC has the authority to grant a specific license for a ransomware victim to make a payment to an SDN or other blocked person,[223] but the OFAC Advisory confirms that is unlikely.[224] In addition, no general license or regulatory exemption from prosecution currently exists for making a ransom payment.[225]

The OFAC Advisory does encourage victims and those assisting them with ransomware attacks to report the attacks to various government agencies and cybersecurity offices, and to "contact OFAC if there is any reason to suspect a potential sanctions nexus with regard to a ransomware payment."[226]

---

218. Collins et al., *supra* note 201 (noting that OFAC discretion also extends to determination of penalties).

219. OFF. OF FOREIGN ASSETS CONTROL, U.S. DEP'T OF THE TREASURY, *supra* note 26, at 5 (updating the October 1, 2020, advisory to broaden the agencies to which reports may be made).

220. *Id.* at 4–5.

221. The OFAC Advisory specifies that credit for reporting to law enforcement or other relevant agencies is available "in the case of ransomware payments that may have a sanctions nexus." *Id.* at 5.

222. *Id.*

223. *See OFAC License Application Page*, U.S. DEP'T OF THE TREASURY, https://home.treasury.gov/policy-issues/financial-sanctions/ofac-license-application-page (last visited Sept. 21, 2021) (noting that a license is an authorization from OFAC to engage in a transaction that would otherwise be prohibited).

224. OFF. OF FOREIGN ASSETS CONTROL, U.S. DEP'T OF THE TREASURY, *supra* note 26, at 4 (explaining that OFAC will review license applications involving ransomware payments with a presumption of denial).

225. *See* OFF. OF FOREIGN ASSETS CONTROL, U.S. DEP'T OF THE TREASURY, *supra* note 26, at 5 (confirming that applications will be reviewed on a "case-by-case" basis).

226. *Id.*

Even if a license were likely, the current license process is poorly suited to timely assistance. OFAC often takes "weeks if not months" to respond to license requests, and "generally refuses to issue licenses for theoretical or potential scenarios or where U.S. jurisdiction is uncertain."[227] As mentioned, U.S. jurisdiction is likely to be uncertain in most ransomware attacks because hackers often conceal their identity and location.

5. *The Threat of OFAC Enforcement in the Ransomware and Cryptocurrency Context*

Because cryptocurrencies are often held pseudonymously, enforcement of U.S. sanctions and other measures in the ransomware context has been challenging. OFAC has designated a number of hackers and ransomware attackers, and their bitcoin addresses, as SDNs. For example, the OFAC Advisory mentioned Bogachev (responsible for Cryptolocker), a list of Iranians (responsible for the SamSam ransomware used against the City of Atlanta, the Colorado Department of Transportation, and a number of health companies), the North Korean Lazarus Group (responsible for WannaCry 2.0), and Evil Corp. (responsible for the ransomware used against a number of banks and other attacks).[228] In addition, on September 21, 2021, OFAC designated as SDNs the Russia-based cryptocurrency over-the-counter broker SUEX OTC and 25 related Bitcoin, Ether, and Tether addresses for "facilitating financial transactions for ransomware actors."[229] SUEX is thought to have received nearly $13 million from ransomware operators including Ryuk, which was involved in the U.S. Coast Guard cyberattack.[230] The SUEX sanction was OFAC's first designa-

227. *See* Krauland et al., *supra* note 28.

228. OFF. OF FOREIGN ASSETS CONTROL, U.S. DEP'T OF THE TREASURY, *supra* note 26, at 2–3 (noting hackers who have been designated as SDNs).

229. *Publication of Updated Ransomware Advisory; Cyber-related Designation*, U.S. DEP'T OF THE TREASURY (Sept. 21, 2021), https://home.treasury.gov/policy-issues/financial-sanctions/recent-actions/20210921.

230. *Chainalysis in Action: OFAC Sanctions Russian Cryptocurrency OTC Suex that Received Over $160 Million from Ransomware Attackers, Scammers, and Darknet Markets,* CHAINALYSIS INSIGHTS: CHAINALYSIS BLOG (Sept. 21, 2021), https://blog.chainalysis.com/reports/ofac-sanction-suex-september-2021 (detailing some of the illicit payment sources); *Ryuk Ransomware Took Down U.S. Coast Guard Operations,* CISOMAG (Dec. 3, 2019), https://cisomag.eccouncil.org/ryuk-ransomware-took-down-u-s-coast-guard-operations/ (identifying the attack as deploying Ryuk ransomware).

tion of a virtual currency exchange for laundering cyber-ransoms.[231]

As OFAC has added ransomware hackers and bitcoin addresses to its SDN list, the dilemma for ransomware victims who pay has worsened. In 2020, Garmin Corp. reportedly paid a multimillion dollar ransom to Evil Corp.,[232] a Russian cybercriminal gang[233] against which OFAC has imposed sanctions,[234] to regain control of its GPS and smartwatch systems. In 2021, CNA Financial Corp. reportedly paid a $40 million ransom in response to a Phoenix Locker attack.[235] Phoenix Locker is a variant of another ransomware (Hades) created by Evil Corp.[236] At the time, CNA Financial Corp. specifically noted that Phoenix was "[not] on any prohibited party list and [was] not a sanctioned entity" and stated that it had "followed all laws, regulations, and published guidance, including OFAC's 2020 ransomware guidance, in its handling of this matter."[237]

In addition, OFAC is actively enforcing its regulations in the context of cryptocurrency service businesses. In December 2020, OFAC announced a settlement with BitGo, which offers non-custodial digital wallet management services,[238] for providing its digital wallet services to SDNs.[239] OFAC alleged

---

231. Press Release, U.S. Department of the Treasury, Treasury Takes Robust Actions to Counter Ransomware (Sept. 21, 2021), https://home.treasury.gov/news/press-releases/jy0364 (labeling SUEX "complicit" in ransomware activity).

232. Collins et al., *supra* note 201.

233. Hern, *supra* note 89 (explaining that Garmin's smartwatch and GPS business was held hostage for three days).

234. OFF. OF FOREIGN ASSETS CONTROL, U.S. DEP'T OF THE TREASURY, *supra* note 95 (identifying Evil Corp., also known as the Dridex Gang, as an SDN).

235. Brittany Chang, *One of the Biggest US Insurance Companies Reportedly Paid Hackers $40 Million Ransom After a Cyberattack,* BUS. INSIDER (May 22, 2021) https://www.businessinsider.com/cna-financial-hackers-40-million-ransom-cyberattack-2021-5 (updating reports on the CNA attack to indicate a ransom had been paid).

236. *Id.*

237. *Id.* (quoting a CNA spokesperson).

238. *Settlement Agreement between the U.S. Department of the Treasury's Office of Foreign Assets Control and BitGo, Inc.*, U.S. DEP'T OF THE TREASURY (Dec. 30, 2020), https://home.treasury.gov/policy-issues/financial-sanctions/recent-actions/20201230_33 (announcing the settlement).

239. Enforcement Release, U.S. Department of the Treasury, OFAC Enters Into $98,830 Settlement with BitGo, Inc. for Apparent Violations of Mul-

BitGo had reason to know it was providing services to users in sanctioned countries based on their Internet Protocol (IP) addresses.[240]

In February 2021, OFAC settled with BitPay, Inc., which offers payment processing solutions for merchants to accept digital currency,[241] for 2,102 apparent violations of multiple sanctions programs.[242] OFAC alleged that BitPay allowed persons who appear to have been located in sanctioned countries to transact with merchants on BitPay's platform, "even though BitPay had location information, including Internet Protocol (IP) addresses and other location data, about those persons prior to effecting the transactions."[243]

C. *Anti-Money Laundering Liability*

1. *U.S. Measures*

A ransomware payment may also be subject to penalties under U.S. anti-money laundering (AML) regulations. U.S. law prohibits money laundering, which includes various techniques employed by criminals to make illegally obtained funds appear legitimate.[244] U.S. efforts to combat money laundering are based in large part on the AML regulations promulgated pursuant to the legislative framework known as the Bank Secrecy Act, alternatively known as the Currency Transactions

---

tiple Sanctions Programs Related to Digital Currency Transactions (Dec. 30, 2020), https://home.treasury.gov/system/files/126/20201230_bitgo.pdf (specifying that BitGo is based in Palo Alto, California).

240. *Id.*

241. *Settlement Agreement between the U.S. Department of the Treasury's Office of Foreign Assets Control and BitPay, Inc.*, U.S. DEP'T OF THE TREASURY (Feb. 18, 2021), https://home.treasury.gov/policy-issues/financial-sanctions/recent-actions/20210218 (announcing the settlement).

242. Enforcement Release, U.S. Department of the Treasury, OFAC Enters into $507,375 Settlement with BitPay, Inc. for Apparent Violations of Multiple Sanctions Programs Related to Digital Currency Transactions (Feb. 18, 2021), https://home.treasury.gov/system/files/126/20210218_bp.pdf (specifying that BitPay is based in Atlanta, Georgia).

243. U.S. DEP'T OF THE TREASURY, *supra* note 238 (implying that the company had reason to know that certain transactions were with persons in sanctioned countries).

244. *What Is Anti-Money Laundering?*, CORP. FIN. INST., https://corporatefinanceinstitute.com/resources/knowledge/finance/anti-money-laundering/ (last visited Jul. 31, 2021).

Reporting Act of 1970,[245] as amended by in 2001 by the USA PATRIOT Act[246] and the Anti-Money Laundering Act of 2020 (AMLA).[247] AML regulation is designed to detect, deter, and disrupt terrorist financing[248] and other criminal networks by imposing a variety of recordkeeping and reporting requirements on certain persons usually necessary to some part of the money laundering process.[249]

Some of the primary responsibilities imposed by AML regulations are know-your-customer requirements which require all financial institutions to conduct customer due diligence.[250] Customer due diligence includes identifying and verifying the identity of customers and their beneficial owners (when cus-

245. 31 U.S.C. §§ 5311–32. The Currency and Financial Transactions Reporting Act of 1970 was "designed to help identify the source, volume and movement of currency and other monetary instruments transported or transmitted into or out of the U.S." Julie Stackhouse, *What Is the Bank Secrecy Act and Why Does It Exist?,* FED. RSRV. BANK OF ST. LOUIS: ON THE ECON. BLOG (Apr. 23, 2018), https://www.stlouisfed.org/on-the-economy/2018/april/what-bank-secrecy-act-why-exist (explaining that Congress was concerned about cash coming in and out of the country).

246. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001, 107 Pub. L. No. 56, 115 Stat. 272 (codified in scattered sections of U.S.C.) (strengthening U.S. measures to prevent international money laundering and the financing of terrorism).

247. AMLA was enacted as part of the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021. William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, Pub. L. No. 116-283, §§ 6001–511, 134 Stat. 3388, 4547–633. AMLA modernized AML by specifying new standards for testing the technology and processes used for AML compliance, with the challenge of cryptocurrencies in mind. Carl F. Fornaris et al., *The Anti-Money Laundering Act of 2020: Congress Enacts the Most Sweeping AML Legislation Since Passage of the USA PATRIOT Act,* NAT'L L. REV. (Jan. 19, 2021), https://www.natlawreview.com/article/anti-money-laundering-act-2020-congress-enacts-most-sweeping-aml-legislation-passage (explaining that the Act was passed as part of the National Defense Authorization Act for Fiscal Year 2021, over then-President Trump's veto).

248. *Bank Secrecy Act (BSA) & Related Regulations,* OFF. OF THE COMPTROLLER OF THE CURRENCY, https://www.occ.gov/topics/supervision-and-examination/bsa/bsa-related-regulations/index-bsa-and-related-regulations.html (last visited Jul. 31, 2021).

249. *See* 31 U.S.C. § 5311 (identifying the purpose of the subchapter as requiring reports and records that help in criminal, tax, or regulatory investigations or proceedings, and that help in conducting intelligence or counterintelligence activities to protect against terrorism).

250. 31 C.F.R. § 1010.230 (2021).

tomers are legal entities), understanding the nature and purpose of customer relationships, and ongoing monitoring to maintain and update customer information and identify suspicious transactions.[251]

AML regulations also require filing of Currency Transaction Reports (CTRs) when there are cash or coin transactions over $10,000 conducted by or for one person, or multiple currency transactions that total over $10,000 in a single day.[252] In addition, AML regulations require Suspicious Activity Reports (SARs) to be filed when, for example, transactions totaling $5,000 or more are known or suspected to involve funds derived from illegal activities.[253] Failure to comply with the customer due diligence requirements or to file CTRs and SARs can result in severe civil and criminal penalties.[254] AMLA enhanced criminal penalties, adding sanctions against intentionally deceiving or withholding information from financial institutions.[255]

2. *Enforcement of AML Laws*

Most AML regulations apply to "financial institutions," which include banks, broker/dealers, "money services busi-

---

251. *Id.* at § 1010.230(b).

252. *Id.* at §§ 1010.311, 1010.314(b). *See also Notice to Customers: A CTR Reference Guide*, U.S DEP'T OF THE TREASURY FIN. CRIMES ENF'T NETWORK, https://www.fincen.gov/sites/default/files/shared/CTRPamphlet.pdf (last visited Jul. 15, 2020) (noting CTR requirements for personal identification information about the individual conducting the transaction including social security numbers, driver's licenses, or other government issued documents).

253. 12 C.F.R. § 21.11(c)(2) (2021).

254. 31 C.F.R. § 1022.380(e). For rules concerning enforcement, penalties, and forfeiture, see 31 C.F.R. §§ 1010.810–850. Government enforcement has included a multi-billion-dollar 2020 settlement with Goldman Sachs for, *inter alia,* AML compliance violations. *Goldman Sachs Fined $2.9B*, BANKERS ONLINE (Oct. 23, 2020), https://www.bankersonline.com/topstory/166119 (noting that the Federal Reserve Board assessed a $154 million civil penalty for Goldman's failure to maintain appropriate oversight, internal controls, and risk management in connection with its 1MDB transactions).

255. Kevin M. Bolan et al., *The Anti-Money Laundering Act of 2020–Expanding Anti-Money Laundering Reporting Responsibilities to Small Businesses*, WHITE & CASE (Feb. 16, 2021), https://www.whitecase.com/publications/alert/anti-money-laundering-act-2020-expanding-anti-money-laundering-reporting (explaining the new penalties).

nesses," and a variety of other actors.[256] "Money services businesses" are defined as persons doing business as, among other things, foreign exchange dealers, check cashers, traveler's check and money order issuers, and "money transmitters."[257] In turn, "money transmission services" are defined as "the acceptance of currency, funds, or other value that substitutes for currency from one person *and* the transmission of currency, funds, or other value that substitutes for currency to another location or person or by any means."[258]

AML regulations are not limited to U.S. financial institutions and money services businesses. They also apply to all other U.S. persons; U.S. branches of foreign financial institutions; non-U.S. financial institutions with certain U.S.-based operations; and non-U.S. financial institutions with transactions processed through a U.S. financial institution, or with operations affected by U.S. sanctions.[259]

AML measures are enforced by FinCEN, which, like the OFAC, is part of the Department of the Treasury.[260] FinCEN's mission is "to safeguard the financial system from illicit use and combat money laundering and promote national security through the collection, analysis, and dissemination of financial intelligence and strategic use of financial authorities."[261] FinCEN receives and maintains financial transactions data,

256. Other actors include, for example, telegraph companies, casinos, card clubs, and commodities brokers. 31 C.F.R. § 1010.100(t).

257. *Id.* at § 1010.100(ff).

258. *Id.* at § 1010.100(ff)(5)(i) (emphasis added). AMLA codified existing FinCEN guidance, which had included cryptocurrencies as "value that substitutes for currency" for purposes of the definition of money services businesses since 2013.

259. *Who is Subject to US AML Laws?*, WILLKIE COMPLIANCE CONCOURSE, https://complianceconcourse.willkie.com/resources/anti-money-laundering-us-who-is-subject-to-us-aml-laws (last visited July 15, 2021) (noting that all institutions subject to FinCEN regulation are required to maintain risk-based compliance programs).

260. *See About*, U.S. DEP'T OF THE TREASURY, https://home.treasury.gov/about/general-information (last visited Sept. 21, 2021) (listing the offices and bureaus of the department).

261. *What We Do*, FIN. CRIMES ENF'T NETWORK, U.S DEP'T OF THE TREASURY, https://www.fincen.gov/what-we-do#:~:text=FinCEN%20is%20a%20bureau%20of%20the%20U.S.%20Department%20of%20the%20Treasury.&text=finCEN's%20mission%20is%20to%20safeguard,strategic%20use%20of%20financial%20authorities (last visited July 15, 2021) (explaining FinCEN's duties and responsibilities).

which it analyzes and disseminates for law enforcement purposes.[262]

3. *AML Laws in the Ransomware Context*

In 2020 and 2021, FinCEN issued and updated an advisory on ransomware and the facilitation of ransom payments (the FinCEN Advisory), warning that a ransomware victim who pays the ransom, and those who assist the victim, may face prosecution for violation of AML regulations.[263]

The FinCEN Advisory made it clear that financial institutions need to file SARs when handling ransomware payments.[264] In the same vein, the FinCEN Advisory noted that others who assist with a ransom payment might also face liability.[265] For example, incident response companies and cyber insurance companies who exchange a ransomware victim's funds for cryptocurrencies and then transfer that cryptocurrency to the ransomware attacker's accounts may be engaging in "money transmission."[266] As discussed above, money transmitters in the United States constitute "money services businesses," and therefore are "financial institutions" subject to the AML regulations.[267] Among other things, those regulations require registration with FinCEN, adoption of a written AML compliance program with adequate policies and procedures, designation of a chief compliance officer, training for appropriate personnel, and independent testing of the compliance program.[268] In addition, financial institutions are required to file SARs for transactions that raise red flags.[269] The FinCEN Advisory listed some potential indicators of ransomware and associated money laundering.[270] Red flags include, for example, situations in which a customer receives funds and then, shortly afterwards, transfers the same amount to a cryptocurrency exchange.[271] In addition, the FinCEN Advisory identi-

262. *Id.*
263. FIN. CRIMES ENF'T NETWORK, *supra* note 23, at 4.
264. *Id.* at 8–9.
265. *Id.* at 4.
266. *Id.*
267. *See* discussion *infra*, Section III.C.2.
268. Krauland et al., *supra* note 28.
269. FIN. CRIMES ENF'T NETWORK, *supra* note 23, at 7.
270. *Id.*
271. *Id.* at 8 (noting red flag indicator no. 5).

fied four sectors at high risk for ransomware attacks—government, finance, education, and healthcare—and advised financial institutions to look for transactions between customers in those sectors, and digital forensics and incident response or cyber insurance companies.[272] FinCEN warned that it "will not hesitate to take action against entities and individuals engaged in money transmission or other [money services business] activities if they fail to register with FinCEN or comply with their other AML obligations."[273]

4. *The Threat of AML Enforcement in the Ransomware Context*

So far, financial institutions and payment providers have faced the most risk of AML liability in the ransomware context.[274] In 2017, FinCEN assessed a $110 million civil money penalty for AML violations by virtual currency exchange BTC-e,[275] and a $12 million penalty against one of its operators, a Russian national who was arrested in Greece for his role in the violations.[276] Among other things, FinCEN found that BTC-e facilitated over $3 million in transactions tied to ransomware attacks, including CryptoLocker and Locky.[277]

5. *Stricter Regulations May Be on the Way for Cryptocurrency Transactions*

Regulators are in the process of examining the role of cryptocurrencies in recent hacks.[278] In late 2020, FinCEN and the U.S. Federal Reserve proposed several measures that will increase the scope of AML rules and liability in the ran-

272. *Id.* at 7 (noting red flag indicator no. 4).

273. *Id.* at 4.

274. *See* Silver et al., *supra* note 5.

275. Press Release, Financial Crimes Enforcement Network, United States Department of the Treasury, FinCEN Fines BTC-e Virtual Currency Exchange $110 Million for Facilitating Ransomware, Dark Net Drug Sales (July 26, 2017), https://www.fincen.gov/news/news-releases/fincen-fines-btc-e-virtual-currency-exchange-110-million-facilitating-ransomware (announcing the penalty).

276. *Id.*

277. *Id.*

278. David Uberti & James Rundle, *U.S. Looks into Cryptocurrency's Role in Ransomware Hacks*, WALL ST. J. (June 3, 2021, 6:34 PM), https://www.wsj.com/articles/u-s-looks-into-cryptocurrencys-role-in-ransomware-hacks-11622759665 (noting that White House officials are looking for better ways to trace ransomware).

somware payment context. Both proposals have the potential to shift substantial responsibility onto third parties who assist ransomware victims with ransom payments.

One proposed regulation would lower the threshold for recordkeeping and information transmission rules from $3,000 to $250 for fund transfers or transmittals that begin or end outside the United States[279] The revised rule would also clarify that "money" includes cryptocurrency, defined as "a medium of exchange . . . that either has an equivalent value as currency, or acts as a substitute for currency, but lacks legal tender status[,]" as well as "digital assets that have legal tender status."[280]

Another proposed regulation would require financial institutions to report any cryptocurrency transfers worth over $10,000 within fifteen days, and to keep records for any transfers worth over $3,000 if the counterparty uses an unhosted wallet.[281] This proposed regulation has been controversial,

---

279. Threshold for the Requirement to Collect, Retain, and Transmit Information on Funds Transfers and Transmittals of Funds That Begin or End Outside the United States, and Clarification of the Requirement to Collect, Retain, and Transmit Information on Transactions Involving Convertible Virtual Currencies and Digital Assets with Legal Tender Status, 85 Fed. Reg. 68005, 68006 (proposed Oct. 27, 2020) (to be codified at 31 C.F.R. pts. 1010, 1020) (proposing "[l]owering of Threshold From $3,000 to $250 for Funds Transfers and Transmittals of Funds by Financial Institutions That Begin or End Outside the United States"). *See also* Evan Weinberger, *Treasury to Wrap Crypto Anti-Money Laundering Rules by Fall*, BLOOMBERG L. (June 11, 2021), https://news.bloomberglaw.com/securities-law/treasury-to-wrap-crypto-anti-money-laundering-rules-by-fall (outlining the proposal).

280. Threshold for the Requirement to Collect, Retain, and Transmit Information on Funds Transfers and Transmittals of Funds That Begin or End Outside the United States, and Clarification of the Requirement to Collect, Retain, and Transmit Information on Transactions Involving Convertible Virtual Currencies and Digital Assets with Legal Tender Status, 85 Fed. Reg. 68005, 68006 (proposed Oct. 27, 2020) (to be codified at 31 C.F.R. pts. 1010, 1020). The final rule is expected in September 2021. Weinberger, *supra* note 279.

281. Requirements for Certain Transactions Involving Convertible Virtual Currency or Digital Assets, 85 Fed. Reg. 83840, 83848 (proposed Dec. 23, 2020) (to be codified at 31 C.F.R. pts. 1010, 1020, 1022). The rule would require financial institutions to collect and keep records of the type of cryptocurrency, time, transaction value, payment instructions received by the financial institution's customer, any forms provided, name and physical address of each counterparty to the financial institution's customer, any other information to identify the transaction, accounts and (as reasonably

with over 7,000 comment letters filed,[282] including a 46-page objection from Coinbase, the largest cryptocurrency exchange in the United States.[283]

D. *Private Parties May Sue Ransomware Victims and Those Who Assist Them*

Ransomware victims who pay their attackers, and those who assist them with such payments, arguably may also face the possibility of liability under the provisions of the Anti-Terrorism Act (ATA),[284] as amended in 2016 by the Justice Against Sponsors of Terrorism Act (JASTA).[285] ATA and JASTA (together, ATA/JASTA) were enacted to interdict terrorist funding through non-traditional financial services. Although not designed for the ransomware payment context, they provide persons injured by acts of international terrorism with a cause of action against the foreign terrorist organization as well as its sources of funding.[286]

Under ATA/JASTA, U.S. plaintiffs injured by an act of international terrorism may seek treble damages plus costs and attorneys' fees from the terrorist perpetrators and any other person or entity that provided material support or financing

---

available) parties. *Id.* at 83860–61 (proposing changes to 31 C.F.R. § 1010.410). The final rule is expected in November 2021. Weinberger, *supra* note 279.

282. *See* Comments Tab for Requirements for Certain Transactions Involving Convertible Virtual Currency or Digital Assets, REGULATIONS.GOV, https://www.regulations.gov/document/FINCEN-2020-0020-0001/comment (last visited July 31, 2021).

283. Letter from Paul Grewal, Chief Legal Officer, Coinbase, to Pol'y Div., Fin. Crimes Enf't Network (Jan. 4, 2021), https://www.regulations.gov/comment/FINCEN-2020-0020-6205 (criticizing the proposed rule as "bad regulation done poorly").

284. Antiterrorism Act of 1990 § 132, 18 U.S.C. § 2333 (2019).

285. Justice Against Sponsors of Terrorism Act, Pub. L. No. 114-222, 120 Stat. 852 (codified as amended in scattered sections of 18, 28 U.S.C.). The Anti-Terrorism Clarification Act of 2018 made additional changes to the law that are not relevant to this analysis. Anti-Terrorism Clarification Act of 2018, Pub. L. No. 115-253, 132 Stat. 3183 (codified as amended in scattered sections of 18 U.S.C.).

286. Jamie L. Boucher et al., *The Potential Impact of Terrorism Lawsuits Under the Antiterrorism Act on Ordinary Corporate, Banking and Sovereign Enterprises*, SKADDEN, ARPS, SLATE, MEAGHER & FLOM LLP, (May 26, 2020), https://www.skadden.com/insights/publications/2020/05/the-potential-impact-of-terrorism-lawsuits (explaining the cause of action available to terror victims).

for the attack.[287] To seek secondary liability, the U.S. plaintiff must be injured in a terrorist attack "committed, planned or authorized" by a foreign terrorist organization so-designated at the time of the attack, and the defendant must have conspired with or *aided and abetted* the foreign terrorist organization.[288] "A defendant aids and abets if it was generally aware that it was assuming a role in furthering the [organization's] terrorist attack and that it knowingly and substantially assisted the [organization] that carried out the attacks."[289]

In the past, ATA/JASTA secondary liability claims have been brought against traditional gatekeepers like financial institutions, often following prosecutions for violations of OFAC sanctions.[290] However, the rise of virtual currencies and the expansion of the understanding of money transmitters[291] has broadened the pool of potential ATA/JASTA defendants. In addition, plaintiffs have begun bringing ATA/JASTA civil suits against companies in other industries, "including pharmaceutical companies, government contractors, and social media platforms, for direct or indirect payments or provision of services to terrorist organizations."[292] Thus, ransom payments that make their way, even indirectly, to a foreign terrorist organization that carries out an attack injuring U.S. individuals may result in lawsuits against parties that participated in that financing chain.

E. *A Plethora of Regulatory Recommendations and Guidance*

The warnings in the OFAC and FinCEN advisories are only two of the regulatory responses to the ransomware epidemic. National security is dependent upon the integrity of

---

287. 18 U.S.C. §§ 2333(a), (d)(2).

288. *Id.* § 2333(d)(2). A foreign terrorist organization is a foreign-based organization that engages in terrorist activity threatening the security of U.S. nationals or U.S. national security. 8 U.S.C. § 1189 (2019) (providing the process for designation under the Immigration and Nationality Act).

289. Alexis Collins et al., *Cryptocurrency and Other New Forms of Financial Technology: Potential Terrorist Concerns and Liability*, CLEARY GOTTLIEB 3 (June 25, 2021), https://www.clearygottlieb.com/-/media/files/alert-memos-2021/2021_06_25-terrorist-financing-concerns-and-liability-in-cryptocurrency-and-fintech-pdf.pdf (discussing the required U.S. nexus).

290. *Id.* at 3–5 (including examples).

291. *See generally* discussion *supra* Section III.C.

292. Collins et al., *supra* note 289, at 4 (providing specific examples of litigation).

digital platforms,[293] and such platforms exist across society, subject to a host of different legal authorities.[294] Depending on the sector in which it operates, a ransomware victim may find itself coping with recommendations and requirements from multiple sources. Our hypothetical hospital might be looking at guidance from, to name just a few examples:

- Department of Homeland Security, particularly its Cybersecurity and Infrastructure Security Agency (CISA);[295]
- Department of Health and Human Services;[296]
- National Cyber Investigative Joint Task Force;[297]
- Department of Justice Ransomware and Digital Extortion Task Force;[298]

---

293. Statement of Downing, *supra* note 15 (arguing that ransomware is a threat to national security).

294. See, for example, the list that follows in the text.

295. HOMELAND SECURITY, https://www.dhs.gov (last visited July 22, 2021) (including news and updates on cybersecurity requirements); *Stop Ransomware,* CISA, CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY, https://www.cisa.gov/stopransomware (last visited July 22, 2021) (providing alerts, guidance, resources, and instructions for reporting ransomware).

296. *Fact Sheet: Ransomware and HIPAA*, OFF. FOR CIV. RTS., U.S. DEP'T OF HEALTH & HUM. SERVS. (July 11, 2016), https://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf (explaining how HIPAA compliance can help covered entities prevent and recover from ransomware).

297. *Ransomware: What It Is & What To Do About It,* NAT'L CYBER INVESTIGATIVE JOINT TASK FORCE, INTERNET CRIME COMPLAINT CTR. (IC3), https://www.ic3.gov/Content/PDF/Ransomware_Fact_Sheet.pdf (last visited Oct. 24, 2021) (listing 10 government agencies or offices as participants in the task force); *see also*, Press Release, Federal Bureau of Investigation, The National Cyber Investigative Joint Task Force Releases Ransomware Fact Sheet (Feb. 4, 2021), https://www.fbi.gov/news/pressrel/press-releases/the-national-cyber-investigative-joint-task-force-releases-ransomware-fact-sheet (announcing release of the fact sheet); *What We Investigate*, NAT'L CYBER INVESTIGATIVE JOINT TASK FORCE, https://www.fbi.gov/investigate/cyber/national-cyber-investigative-joint-task-force (explaining the origins, composition, and mandate of the task force).

298. *Memorandum for All Federal Prosecutors: Guidance Regarding Investigations and Cases Related to Ransomware and Digital Extortion*, Off. of the Deputy Att'y Gen., U.S. Dep't of Just. (June 3, 2021), https://www.justice.gov/dag/page/file/1401231/download (setting out notification requirements for DOJ divisions). *See also* Dustin Volz, *Ransomware Targeted by New Justice Department Task Force*, WALL ST. J. (Apr. 21, 2021), https://www.wsj.com/articles/ransomware-targeted-by-new-justice-department-task-force-11619014158 (reporting that the task force includes members of the department's criminal, na-

- Federal Trade Commission;[299]
- Institute for Security and Technology Ransomware Task Force;[300] and
- Center for Internet Security, including its Multi-State Information Sharing and Analysis Center.[301]

The threat of prosecution, added to the "noise" of multiple guidelines,[302] may be confusing for many ransomware victims. In the meantime, attacks continue.

III.
THE DECISION TO PAY A RANSOM

A. *Time Pressure and Uncertainty*

In many cases, hackers begin stealing data on a victim's customers, or patients, or business operations, days or weeks before the ransomware is detected or a ransom demanded.[303] Victims often have to respond to an announced attack

---

tional security, and civil divisions as well as the FBI and the Executive Office of U.S. Attorneys).

299. *Ransomware,* FED. TRADE COMM'N, https://www.ftc.gov/tips-advice/business-center/small-businesses/cybersecurity/ransomware (last visited July 21, 2021) (including suggestions about how to protect businesses and what to do during an attack).

300. RANSOMWARE TASK FORCE, INST. FOR SEC. & TECH., *supra* note 107, at 3 (report by "a team of more than 60 experts from software companies, cybersecurity vendors, government agencies, non-profits, and academic institutions").

301. *Security Primer – Ransomware,* CIS CTR. FOR INTERNET SEC., https://www.cisecurity.org/white-papers/security-primer-ransomware/(last date visited Oct. 24, 2021) (providing recommendations to mitigate ransomware risk). *See also,* MULTI-STATE INFO. SHARING & ANALYSIS CTR., RANSOMWARE GUIDE (2020), https://www.cisa.gov/sites/default/files/publications/CISA_MS-ISAC_Ransomware%20Guide_S508C_.pdf (listing ransomware best practices).

302. RANSOMWARE TASK FORCE, INST. FOR SEC. & TECH., *supra* note 107, at 35 (calling the number of guides and technological tools currently available "confusing and problematic").

303. *See* Liam Tung, *This Is How Long Hackers Will Hide in Your Network Before Deploying Ransomware or Being Spotted*, ZDNET (May 19, 2021), https://www.zdnet.com/article/this-is-how-long-hackers-will-spend-in-your-network-before-deploying-ransomware-or-being-spotted/ (reporting an average of 11 days according to UK security firm Sophos). *See also*, Hobbs, *supra* note 58*;* Heather Landi, *Before Attacking IT Systems, Hackers Stole Information from 147K Patients, Scripps Says,* FIERCE HEALTHCARE (June 3, 2021), https://www.fiercehealthcare.com/tech/before-attacking-it-systems-hackers-stole-information-from-147-000-patients-scripps-health; Kochman, *supra* note 54

quickly,[304] while operating in panic mode.[305] As discussed above, victims who pay the ransom are "generally forced to do so without a clear understanding of the recipient."[306] Ransomware attackers do not give the victim time to get a firm handle on the scope of the problem.

B. *Arguments Against Paying*

The U.S. government advises against paying ransoms,[307] and, as discussed above, some agencies have emphasized potential liability for payment. Paying a ransom tends to increase the risk of cyberattacks to others.[308] A successful ransomware attack presumably encourages the attacker. Moreover, the ransom provides funds that may enable[309] the hackers to target others, including customers and suppliers of the ransomware victim.[310] Paying up may also "encourage other criminal actors to engage in the distribution of ransomware, and/or fund illicit activities."[311] As the business of ransomware continues, prices are rising.[312] Between 2019 and 2020, the average ran-

---

(noting that cybercriminals steal sensitive data before locking victims out and demanding ransoms).

304. *See, e.g.*, Joe Panattieri, *Colonial Pipeline Cyberattack: Timeline and Ransomware Attack Recovery Details,* MSSP ALERT (June 7, 2021), https://www.msspalert.com/cybersecurity-breaches-and-attacks/ransomware/colonial-pipeline-investigation/ (setting out the timeline for the pipeline attack). *See also* Krauland et al., *supra* note 28 (noting the tight timetables usually associated with an attack).

305. Mark Lanterman, *Ransomware and Federal Sanctions,* 78 BENCH & BAR MINN. 6, 6 (2021) (noting that victims want the incident to be resolved at any cost and many rush to pay the cyberterrorist).

306. *See* Krauland et al., *supra* note 28.

307. CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY ET AL., JOINT CYBERSECURITY ADVISORY 16 (2020), https://us-cert.cisa.gov/ncas/alerts/aa20-302a; OFF. OF FOREIGN ASSETS CONTROL, U.S. DEP'T OF THE TREASURY, *supra* note 25 (strongly discouraging payment of ransom demands).

308. RANSOMWARE TASK FORCE, INST. FOR SEC. & TECH., *supra* note 107, at 49.

309. *See also* N.Y. STATE DEP'T OF FIN. SERVS., *supra* note 183 (stating that cybercriminals use ransomware to fund more frequent and sophisticated attacks).

310. Silver et al., *supra* note 5.

311. FED. BUREAU OF INVESTIGATION, *supra* note 11, at 14 (claiming that payment may embolden adversaries).

312. Hobbs, *supra* note 58 (noting that average ransom payments across all industries have climbed in recent years).

somware payment rose 33% to $111,605,[313] and demands in 2021 have also been steep.[314]

To add to the confusion, paying a ransom may not prevent loss or disclosure of the ransomware victim's data.[315] Cybersecurity experts estimate that over a quarter of ransomware victims who pay do not recover all of their data.[316] For example, in 2016, Kansas Heart Hospital paid a cyberattack ransom and received a demand for more money instead of a decryption key.[317] The hospital declined to pay the second time.[318] One survey found that in nearly 40% of cases in which the ransomware victim paid the ransom, the hackers made a separate demand for additional payment.[319]

Some cyberattacks are purely destructive, and some ransom messages are a ruse.[320] NotPetya was reportedly developed as a disk-wiping cyber-weapon by the Russian military,[321]

---

313. Peter A. Halprin & Nicholas A. Pappas, *Ransomware, Security, and Insurance*, WESTLAW TODAY (May 11, 2021), https://today.westlaw.com/Document/I5de97a99b26711ebbea4f0dc9fb69570/View/FullText.html?transitionType=default&contextData=(sc.Default)&firstPage=true (noting that costs are rising).

314. Silver et al., *supra* note 5; Glover, *supra* note 48 (noting that the number of attempted attacks by mid-2021 had already exceeded the total number for 2020).

315. FED. BUREAU INVESTIGATION, *supra* note 11, at 14 (noting that payment may not restore a victim's data).

316. CYBER-EDGE GRP., 2021 CYBERTHREAT DEFENSE REPORT 3 (2021), https://cyber-edge.com/cdr/ (showing that 72% of ransomware victims who pay recover their data).

317. Bill Siwicki, *Ransomware Attackers Collect Ransom from Kansas Hospital, Don't Unlock All the Data, Then Demand More Money,* HEALTHCARE IT NEWS (May 23, 2016), https://www.healthcareitnews.com/news/kansas-hospital-hit-ransomware-pays-then-attackers-demand-second-ransom (discussing the hospital attack).

318. *Id.* (noting the hospital claimed to have paid only a small amount).

319. Ben Kochman, *Regulators Are Homing In on Perils of Ransomware Payments*, LAW360 (Feb. 12, 2021) https://www.law360.com/articles/1354297/regulators-are-homing-in-on-perils-of-ransomware-payouts (citing a survey released by cybersecurity company Proofpoint).

320. *See* Alfred Ng, *US: Russia's NotPetya the Most Destructive Cyberattack Ever,* CNET (Feb. 15, 2018), https://www.cnet.com/tech/services-and-software/uk-said-russia-is-behind-destructive-2017-cyberattack-in-ukraine/ (noting that the ransomware was a disguise for an attack meant to destroy data and cause chaos).

321. *See* Danny Palmer, *Ransomware: The Key Message Maersk Learned from Battling the NonPetya Attack,* ZDNET (Apr. 29, 2019), https://www.zdnet.com/article/ransomware-the-key-lesson-maersk-learned-from-battling-the-

and no key existed to restore a system that suffered an attack using that malware.[322] NotPetya attacks were so destructive that a number of insurance companies denied insurance claims by targeted policyholders, arguing that the cyberattacks were "hostile or warlike action[s]" excluded from coverage.[323]

C. *Paying the Ransom: Risks to the Entity and Its Stakeholders*

A number of factors can influence whether victims agree to pay the ransom demand, including the risk confronted by the entity and other stakeholders. An entity with full offsite data backup, for example, may be more likely to take a principled stand and refuse to pay.[324]

But, in some cases, principled decisions and business decisions do not align.[325] An entity without cyber insurance, or one that is looking at a full system outage, may agree to pay.[326] Given a threat to patient safety,[327] healthcare entities are considered likely to pay.[328] The possibility of data exfiltration may

---

notpetya-attack/ (emphasizing the importance of a strong data recovery process); Press Release, U.S. Department of the Treasury, Treasury Sanctions Russia with Sweeping New Sanctions Authority (Apr. 15, 2021), https://home.treasury.gov/news/press-releases/jy0127 (attributing the attack to Russia's main intelligence agency).

322. Daniel Garrie & Peter A. Halprin, *Placing Ransomware in Context and Avoiding Liability for Paying Ransomware Claims,* 24 J. INTERNET L. 15, 16 (2021) (examining the war exclusion in insurance policies).

323. Adam Santariano & Nicole Perlroth, *Big Companies Thought Insurance Covered a Cyberattack. They May Be Wrong*, N.Y. TIMES (Apr. 15, 2019), https://www.nytimes.com/2019/04/15/technology/cyberinsurance-notpetya-attack.html (discussing suits filed by against insurers in U.S. courts over the war exclusion and damages from NotPetya attacks).

324. *See* Custers et al., *supra* note 42.

325. Kochman, *supra* note 319 (quoting cybersecurity attorney Jena Valdetero).

326. RANSOMWARE TASK FORCE, INST. FOR SEC. & TECH., *supra* note 107, at 12 (discussing factors influencing decisions to pay).

327. Deborah R. Farringer, *Send Us the Bitcoin or Patients Will Die: Addressing the Risks of Ransomware Attacks on Hospitals,* 40 SEATTLE U. L. REV. 937, 939–40 (2017).

328. Shawn Rice, *Cyberattack Class Suits Have Unpredictable Insurance Impact*, LAW360 (June 30, 2020), https://www.law360.com/articles/1399182/cyber-attack-class-suits-have-unpredictable-insurance-impact (quoting Michael Miguel claiming that hospitals often cannot operate without the encrypted data and "don't have the luxury to wait it out and not pay the ransom").

also make an entity more likely to pay.[329] By the end of 2020, most ransomware attacks included this type of double extortion.[330] Data breaches can have substantial ripple effects on other companies or individuals.[331]

Ransomware victims who have refused to pay provide a number of highly publicized cautionary tales. When MedStar Health hospital system suffered a SamSam ransomware attack in 2016, MedStar chose not to pay the ransom.[332] With its computer systems shut down,[333] Medstar's emergency room facilities backed up (leading to delays and confusion).[334] Hospital

---

329. RANSOMWARE TASK FORCE, INST. FOR SEC. & TECH., *supra* note 107, at 12 (explaining that "the theft and threat of public disclosure of sensitive data," known as data exfiltration, or double extortion, intensifies pressure on victims).

330. COVEWARE, *supra* note 179.

331. *See* Krauland et al., *supra* note 28 (noting a ransom payment decision requires consideration of the victim's operations, and the risk to stakeholders).

332. Morgan Eichensehr, *MedStar Lauds Federal Investigators After Hackers Indicted for 2016 Attack,* BALTIMORE BUS. J. (Nov. 29, 2018), https://www.bizjournals.com/baltimore/news/2018/11/29/medstar-lauds-federal-investigators-after-hackers.html (noting that the hackers had demanded 45 Bitcoins, at the time worth $19,000).

333. Jack Gillum et al., *MedStar Paralyzed as Hackers Take Aim at Another US Hospital,* AP NEWS (Mar. 29, 2016), https://apnews.com/article/c61f2be0d0814595b9006239942a40be (describing hospital operations as "crippled").

334. Ian Duncan & Andrea K. McDaniels, *MedStar Hack Shows Risks that Come with Electronic Health Records*, BALTIMORE SUN (Apr. 2, 2016), https://www.baltimoresun.com/health/bs-md-medstar-healthcare-hack-20160402-story.html (calling MedStar computer systems "crippled").

> MedStar Health patients were being turned away or treated without important computer records Tuesday as the health-care giant worked to restore online systems crippled by a virus. By Tuesday evening, MedStar staff could read — but not update — thousands of patient records in its central database, though other systems remained dark, a spokeswoman said.

John Woodrow Cox, *MedStar Health Turns Away Patients After Likely Ransomware Cyberattack*, WASH. POST (Mar. 29, 2016), https://www.washingtonpost.com/local/medstar-health-turns-away-patients-one-day-after-cyberattack-on-its-computers/2016/03/29/252626ae-f5bc-11e5-a3ce-f06b5ba21f33_story.html.

staff were deprived of critical directions and health history when they administered medication.[335]

In 2018, the City of Atlanta declined to (or, given the timetable, was unable to) pay hackers roughly $50,000 in bitcoin to decrypt its networks after a SamSam ransomware[336] attack.[337] The city's efforts to respond are estimated to have cost more than $2.7 million.[338] In May 2019, the City of Baltimore refused to pay attackers a $76,000 ransom; the cost of the attack has been estimated to be over $18 million.[339] The University of Vermont Health Network took a principled stand against payment after an October 2020 ransomware attack, even though the attack was estimated to cost $1.5 million each

---

335. Kenneth N. Rashbaum, *MedStar Health Cyberattack: Treatment and Patient Safety Impact*, BARTON (Sep. 4, 2019), https://www.bartonesq.com/news-article/medstar-health-cyberattack-treatment-and-patient-safety-impact/.

> A nurse at MedStar Washington Medical Center described the situation as "chaotic," and added that clinicians could not access such vital information as medical history, medications prescribed and drug allergies. A doctor called the problem a "patient safety issue." . . . . One nurse cited a specific example of patient safety, however, stating that an antibiotic with potentially severe side effects had not been stopped within the designated time because of the attack. A physician indicated that laboratory results crucial to determining the best means to treat infection and other conditions could not be quickly processed because of the systems shutdown.

Id.

336. CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY, ALERT AA18-337A, SAMSAM RANSOMWARE (2018), https://us-cert.cisa.gov/ncas/alerts/AA18-337A.

337. *See* Stephen Deere, *U.S. Attorney in Atlanta; City Didn't Pay Cyber Attack Ransom,* ATLANTA JOURNAL-CONSTITUTION (Dec. 5, 2018), https://www.ajc.com/news/crime—law/attorney-atlanta-city-didn-pay-cyber-attack-ransom/CW6cgw1eZfoGAXDRprLzeI/ (reporting on the indictment of two Iranian nationals for the attack).

338. *See* Stephen Deere, *Cost of City of Atlanta's Cyberattack: $2.7 Million – and Rising,* ATLANTA JOURNAL-CONSTITUTION (Apr. 12, 2018), https://www.ajc.com/news/cost-city-atlanta-cyber-attack-million-and-rising/nABZ3K1AXQYvY0vxqfO1FI/ (noting that estimate did not include additional, potentially substantial, costs); Lily Hay Newman, *Atlanta Spent $2.6M to Recover from a $52,000 Ransomware Scare,* WIRED (Apr. 23, 2018), https://www.wired.com/story/atlanta-spent-26m-recover-from-ransomware-scare/ (pointing out the complexity of a ransomware victim's decision to pay).

339. *See* Ian Duncan, *Baltimore Estimates Cost of Ransomware Attack at $18.2 Million as Government Begins to Restore Email Accounts*, BALTIMORE SUN (May 29, 2019), https://www.baltimoresun.com/maryland/baltimore-city/bs-md-ci-ransomware-email-20190529-story.html.

day the system was down.[340] The bill for recovery and lost services was over $63 million,[341] which was reportedly over double the network's insurance coverage.[342]

IV.
A Safe Harbor for Ransomware Preparedness

A. *Problems with Regulatory Action Against Ransomware Victims*

It makes sense to combat terrorism by cutting off the flow of funds to the perpetrators. Still, the threat of liability for making a ransomware payment, without a positive incentive, is unlikely to be sufficient. There are better solutions than forcing ransomware victims to choose between the potentially catastrophic loss of the data stored on their computer network and the possibility of regulatory prosecution. Entities, especially those in high-risk sectors like healthcare, education, and local government, need to take all possible steps to avoid and mitigate exposure to ransomware, but that will not always avoid an attack. Ransomware victims may pay simply because, once they have suffered an attack, they have no other viable option.[343] After all, in 2020, multiple U.S. federal government agencies with (supposedly) the best cybersecurity in the world were the victims of cyberattacks.[344]

---

340. *See* James Rundle, *Ransomware Poses a Threat to National Security, Report Warns*, Wall St. J. (Apr. 29, 2021), https://www.wsj.com/articles/ransomware-now-seen-as-threat-to-national-security-11619728378#:~:text=government%20officials%20and%20cybersecurity%20experts,cartels%20and%20other%20criminal%20organizations (discussing an Institute for Security and Technology report).

341. Erin Brown, *UVM Health Network Cyberattack Fixes Expected to Exceed $63M,* WCAX3 (Dec. 8, 2020), https://www.wcax.com/2020/12/08/uvm-heath-network-cyberattack-fixes-expected-to-exceed-63m/ (noting the financial impacts were still being assessed).

342. Calvin Cutler, *UVM Health Network Continues to Tally Costs of Ransomware Attack*, WCAX3 (Jun. 17, 2021), https://www.wcax.com/2020/12/08/uvm-heath-network-cyberattack-fixes-expected-to-exceed-63m/ (reporting the network was insured for $30 million, and continues to negotiate with its carriers).

343. Silver et al., *supra* note 5.

344. *See* Isabella Jibilian & Katie Canales, *The US Is Readying Sanctions Against Russia over the SolarWinds Cyber Attack. Here Is a Simple Explanation of How the Massive Hack Happened and Why It's Such a Big Deal*, Bus. Insider (Apr. 15, 2021), https://www.businessinsider.com/solarwinds-hack-explained-government-agencies-cyber-security-2020-12 (explaining that the attack, which went undetected for months, enabled the hackers to spy on the

There is some regulatory acknowledgment of the exigency of a ransomware attack and the possibility of payment. In 2016, federal interagency guidance stated that the U.S. government "does not encourage paying a ransom to criminal actors" but understands that executives will evaluate "all options to protect their shareholders, employees, and customers."[345] However, as discussed above, OFAC and FinCEN have articulated a tougher approach to ransomware payments. In fact, some states, including New York,[346] Pennsylvania,[347] North Carolina,[348] and Texas,[349] have even considered legislation banning or restricting ransomware payments.[350]

"upper echelons" of the U.S. Government, including the Department of Homeland Security and the Treasury Department).

345. FED. BUREAU OF INVESTIGATIONS, RANSOMWARE PREVENTION AND RESPONSE FOR CISOS (2016), https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view. *See also*, FED. BUREAU OF INVESTIGATIONS, ALERT NO. I-100219-PSA, HIGH IMPACT RANSOMWARE ATTACKS THREATEN U.S. BUSINESSES AND ORGANIZATIONS (2019), https://www.ic3.gov/Media/Y2019/PSA191002; U.S. DEP'T OF JUST., REPORT OF THE ATTORNEY GENERAL'S CYBER DIGITAL TASK FORCE (2018), https://www.justice.gov/archives/ag/page/file/1076696/download.

346. S. 6154, 2021–22 Leg., Reg. Sess. (N.Y. 2021) (barring state and local taxpayer money from being used to pay a ransom); S. 6806A, 2021–22 Leg., Reg. Sess. (N.Y. 2021) (prohibiting business and healthcare entities, as well as state governmental entities, from paying).

347. S. 726, 2021 Gen. Assemb., Reg. Sess. (Pa. 2021) (prohibiting use of taxpayer money or other public money to pay a ransom). The measure was approved by the Senate Judiciary Committee in June 2021 and moved to the Senate floor. Jenni Bergal, *States Weigh Bans on Ransomware Payoffs,* INS. J. (July 27, 2021), https://www.insurancejournal.com/news/national/2021/07/27/624483.htm.

348. H.R. 813, 2021 Gen. Assemb., Reg. Sess. (N.C. 2021) (prohibiting state agencies and local agencies, including state educational institutions, from paying). The bill passed the House unanimously in May 2021. Benjamin Freed, *North Carolina Moves Toward Ban on Ransomware Payments,* STATESCOOP (May 14, 2021), https://statescoop.com/north-carolina-moves-toward-ban-on-ransomware-payments/.

349. H.R. 3892, 87th Leg., Reg. Sess. (Tex. 2021) (prohibiting government entities or political subdivisions from making ransom payments, but currently moot because the bill died in committee).

350. *State Legislatures Consider Bans on Ransomware Payments,* ALSTON & BIRD PRIV., CYBER & DATA STRATEGY BLOG (June 18, 2021), https://www.alstonprivacy.com/state-legislatures-consider-bans-on-ransomware-payments (noting that bans would fall primarily on state agencies and other local government authorities, though in some cases they could apply more broadly); *see also* Bergal, *supra* note 347 (noting that cybersecurity experts

A better solution would be to recognize both the social costs of paying off criminals and the potential damage of ransomware attacks, and to establish a safe harbor system pursuant to which potential targets could be encouraged to take proactive steps to harden their defenses. In return for these preventive measures, victims could rest assured that, if they do suffer an attack despite their compliance efforts, they could call upon professional or regulatory assistance, and neither they nor those who assist them would face prosecution for paying the ransom if needed. The possibility of assistance and immunity from government prosecution could lead entities to implement the cybersecurity best (or at least much better) practices that have proven elusive to date.[351]

Some related ideas have been floated. An April 2021 report from the Institute for Security and Technology included recommendations including mandating reporting and some immunity for victims who pay.[352] On July 27, 2021, Deputy Assistant Attorney General Richard Downing testified before the Senate Judiciary Committee, suggesting that new legislation might grant ransomware victims some sort of protection in exchange for disclosing an attack to law enforcement.[353] The OFAC Advisory discusses prompt reporting as a potential mitigating factor in its enforcement determinations.[354] A safe harbor solution would shift the emphasis to prevention and would facilitate identification of the ransomware hackers by incentivizing disclosure of cyberattacks.

---

are skeptical about the state initiatives and have warned that the bans could be "catastrophic" for residents).

351. *See* RANSOMWARE TASK FORCE, INST. FOR SEC. & TECH., *supra* note 107, at 18 (indicating that adoption of best practices has been "limited").

352. *Id.* at 47 (recommending mandated reporting of ransom payments in return for a limited form of liability protection in which the reported information "cannot form the basis for a regulatory or other enforcement action."); *see also* discussion *infra* Section V.D.

353. Statement of Downing, *supra* note 15, at 8 (arguing for legislation to make cyberattack reporting mandatory)*; see also* discussion *infra* Section V.D.

354. OFF. OF FOREIGN ASSETS CONTROL, U.S. DEP'T OF THE TREASURY, *supra* note 25, at 5 (also broadening the agencies to which reports may be made to include CISA and Department of the Treasury Office of Cybersecurity and Critical Infrastructure Protection).

Waivers of prosecution because of duress and necessity,[355] and safe harbor rules, are not new to U.S. law. For example, U.S. criminal statutes prohibit material support for terrorism, but in 2015 the DOJ waived the threat of criminal prosecutions for citizens who pay terrorist ransoms.[356] More generally, the law often provides an opportunity for entities to comply with statutory and regulatory safe harbors so that they can be sure their business practices will not be subject to sanctions.[357] Entities receive some measure of certainty in exchange for their voluntary ex ante compliance in furtherance of policy.[358] Federal securities laws enable companies to raise capital in certain circumstances with confidence that registration of the offering is not required.[359] Corporation law has articulated the steps a corporation can employ to gain the protection of a lenient business judgment rule-based review for transactions in which a director has a conflict of interest.[360] In the healthcare sector, there are substantial safe harbor regulations under anti-kickback rules and rules regarding beneficiary inducements.[361] The bankruptcy code includes a safe harbor for certain securities transaction payments, which are exempted from avoidance

355. In criminal law, the defenses of necessity and duress rest on the idea that it is better for society that the defendant choose the lesser evil—violating the law but avoiding the greater evil being threatened. *See* Monu Bedi, *Excusing Behavior: Reclassifying the Federal Common Law Defenses of Duress and Necessity Relying on the Victim's Role,* 101 J. CRIM. L. & CRIMINOLOGY 575, 577–78 (2011) (surveying how federal courts have treated duress and necessity defenses).

356. Press Release, U.S. Dep't of Just., Department of Justice Statement on U.S. Citizens Taken Hostage Abroad (June 24, 2015), https://www.justice.gov/opa/pr/department-justice-statement-us-citizens-taken-hostage-abroad (recognizing the "extraordinarily difficult circumstances" being endured by hostages' families).

357. *See, e.g.*, *Safe Harbor*, CORP. FIN. INST., https://corporatefinanceinstitute.com/resources/knowledge/other/safe-harbor/ (last visited Oct. 24, 2021) (defining the term and providing several examples); Peter P. Swire, *Safe Harbors and a Proposal to Improve the Community Reinvestment Act,* 79 VA L. REV. 349, 370–72 (1993) (analyzing the safe harbor mechanism).

358. Swire, *supra* note 357, at 370.

359. *See, e.g.*, 17 C.F.R. § 230.500 (2012) (known as "Regulation D").

360. *See, e.g.*, MODEL BUS. CORP. ACT, § 8.61 (AM. BAR ASS'N 2016) (outlining requirements for Director's Conflicting Interest Transactions).

361. *See, e.g.*, 42 C.F.R. §§ 1001, 1003 (providing background for revisions to the safe harbors).

by the bankruptcy trustee.[362] By creating a clear safe harbor that would allow ransom payments under certain circumstances without fear of prosecution, regulators could make such attacks harder, thereby protecting not only individuals and institutions, but the digital infrastructure itself.

B. *Hardening Potential Targets*

1. *Operational Measures*

There are a number of operational measures that potential ransomware targets can be encouraged to take in order to avail themselves of the safe harbor. They may include, for example:

- *Assessing Data*: Development of a unified view of the network (what information and programs they have and where they are located), along with regular vulnerability scanning, enables entities to reduce clutter and spot vulnerabilities.[363] Knowing what vital information is being stored, and where, can help determine what to back up.
- *Backing Up*: Depending on the scale of the potential ransomware victim, establishment of multiple rotating backups of critical data, at least one off-site, may be needed.[364] In some cases, experts may recommend an offline and encrypted backup of all data.[365]

---

362. Sections 546(e) and (g) of the Bankruptcy Code prohibit the avoidance and recovery of preferential and constructively fraudulent transfers made in connection with forward contracts and swap agreements. 11 U.S.C. § 546(e), (g).

363. *America Under Cyber Siege: Preventing and Responding to Ransomware Attacks: Hearing Before the S. Comm. on the Judiciary*, 117th Cong. 5 (2021) (statement of Eric Goldstein, Executive Assistant Director for Cybersecurity, U.S. Dept. of Homeland Sec.) [hereinafter statement of Goldstein].

364. *Security Tip (ST19-001): Protecting Against Ransomware*, U.S. DEPT. OF HOMELAND SEC. CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY (Sept. 2, 2021), https://us-cert.cisa.gov/ncas/tips/ST19-001 ("Best practice is to store your backups on a separate device that cannot be accessed from a network, such as on an external hard drive. Once the backup is completed, make sure to disconnect the external hard drive, or separate device from the network or computer.")

365. *See, e.g.*, statement of Goldstein, *supra* note 363, at 4 ("[W]e encourage our partners to maintain offline and encrypted backups of data; conduct regular vulnerability scanning to identify and address vulnerabilities; regularly patch and update software and operating systems, including

- *Updating and Blocking*: A commitment to keeping operating systems, browsers, and security software up-to-date to maintain current patch levels may also be advisable.[366] This may include ad-blocking software and strong filters, intrusion detection systems,[367] and configuring firewalls to block access to known malicious addresses and sites.[368] Anti-virus and anti-malware programs can be set to conduct regular scans automatically.[369]
- *Controlling Access*: Controlling access to the system using whitelisting and limits on user rights may help.[370] Potential victims may only grant privileges necessary to perform assigned tasks. With the rise of remote work, multi-factor authentication can be required for offsite access to network files or applications, using at least two of the three common verifications: something users know (like a password), something users possess (like a token), and something users are (like a fingerprint).

No amount of cybersecurity improvement will address all of the vulnerabilities in the digital ecosystem,[371] but implementing better security technology, combined with other measures, can help.

---

antivirus and anti-malware software; implement a cybersecurity user awareness and training program, including guidance on identifying and reporting suspicious activity; and implement an intrusion detection system (IDS) to detect command and control activity.").

366. *Security Tip (ST19-001): Protecting Against Ransomware*, *supra* note 364.

367. *See, e.g.*, statement of Goldstein, *supra* note 363, at 4.

368. *How to Protect Your Networks from Ransomware*, FED. BUREAU OF INVESTIGATION, https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view (last visited Oct. 24. 2021).

369. *Id.*

370. Ronny Richardson & Max M. North, *Ransomware: Evolution, Mitigation and Prevention*, 13 INT'L MGMT. REV. 10, 16 (2017).

371. *See* Opinion, *Russia's New Form of Organized Crime Is Menacing the World,* N.Y. TIMES (July 31, 2021), https://www.nytimes.com/2021/07/31/opinion/sunday/russia-ransomware-hacking.html (quoting a ransomware expert predicting, "We're not going to defend ourselves out of this problem. . . . We have too many vulnerabilities.").

2. *Employee Training*

Many ransomware attacks exploit human weakness. An employee opens a suspicious email, or clicks on a questionable website, or is somehow tricked into downloading a fraudulent "system update." Many U.S. workers are accustomed to mandatory compliance training; ongoing cybersecurity user awareness can be incorporated into those programs. To avoid ransomware, employees can be trained in, among other things, appropriate password management, social media usage, and identifying and reporting suspicious activity.

In addition, employees can be encouraged to keep the software on their personal devices up-to-date.[372] Those devices are often connected to an organization's network and should be included in the overall ransomware protection plan.[373]

3. *Periodic Audits*

Entities seeking safe harbor status would need to demonstrate their compliance with the safe harbor periodically, with a possibility of audits. Regulators are experienced with the need to keep compliance measures up to date, and periodic examination or reporting can facilitate that process. For example, banks' AML compliance measures are periodically examined.[374] The Department of Health and Human Services' Office of Civil Rights periodically audits selected covered entities and their business associates for their compliance with HIPAA rules.[375] Cybersecurity can employ similar models.

---

372. Mark Adams, *Cyber-Security Basics: Keeping Employee Software Updated*, RED RIVER (Mar. 7, 2019), https://redriver.com/security/cyber-security-basics-software-update-policy (noting that software becomes vulnerable when it is not updated).

373. Danny Palmer, *Ransomware vs. WFH: How Remote Working Is Making Cyberattacks Easier to Pull Off,* ZDNET (Oct. 27, 2020), https://www.zdnet.com/article/ransomware-vs-wfh-how-remote-working-is-making-cyberattacks-easier-to-pull-off/ (discussing the risks created by employees logging onto work networks from home).

374. *See, e.g.*, *BSA/AML Examination Procedures*, FED. FIN. INSTS. EXAMINATION COUNCIL, https://bsaaml.ffiec.gov/examprocedures (last visited Oct. 24, 2021) (providing links to various parts of AML compliance procedure examinations).

375. *HIPAA Privacy, Security, and Breach Notification Audit Program,* U.S. DEP'T OF HEALTH & HUM. SERVS., https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/index.html (last visited Oct. 24,

C. *Cyber Insurance*

1. *Cyber Insurance Controversy*

Cyber insurance has become a focal point in the struggle to deal with ransomware attacks.[376] Many ransomware victims consult their insurance company as part of their response to an attack and hope to rely on that coverage to help them recover their costs from the disruption.

Arguably, however, cyber insurance may invite information asymmetry issues like adverse selection and moral hazard. A potential ransomware victim, knowing it is particularly at risk for a ransomware attack, may seek insurance rather than improve its cybersecurity (adverse selection).[377] For example, in the wake of the Colonial Pipeline ransomware attack, there are allegations that Colonial Pipeline was aware of defects in its cybersecurity.[378] Similarly, once a potential victim has secured cyber insurance, it may engage in risky behavior or forgo recommended cybersecurity improvements or updates (moral hazard).[379] The worry is that neither ransomware victims nor

---

2021). The Health Information Technology for Economic and Clinical Health (HITECH) Act requires such audits. *Id.*

376. In 2016, 26% of insurance clients opted for cyber coverage. That increased to 47% in 2020. U.S. GOV'T ACCOUNTABILITY OFF., GAO-21-477, CYBER INSURANCE: INSURERS AND POLICYHOLDERS FACE CHALLENGES IN AN EVOLVING MARKET 5 (May 20, 2021) (reporting to Congress on the challenges of cyber insurance).

377. *See* Ronen Avraham, *The Economics of Insurance Law—A Primer*, 19 CONN. INS. L.J. 29, 44 (2012) (defining adverse selection as a result of informational asymmetry in which high-risk parties, knowing their "type," seek more insurance coverage than low-risk parties).

378. *See* Alyza Sebenius & Rebecca Kern, *U.S. Lawmakers Chide Colonial Pipeline for Weak Cybersecurity*, BLOOMBERG (June 9, 2021, 2:38 PM) (also noting that the company expected the cost of the ransom to be covered by its cyber insurance); Frank Bajak, *Tech Audit of Colonial Pipeline Found 'Glaring' Problems,* ASSOCIATED PRESS (May 12, 2021), https://apnews.com/article/va-state-wire-technology-business-1f06c091c492c1630471d29a9cf6529d (citing comments from a consulting firm owner who prepared a report on the company's information management practices in 2018). The company is now the subject of a number of lawsuits alleging negligence in its cybersecurity practices. *See* Tim Darnell, *Another Lawsuit Targets Colonial Pipeline After Cyberattack,* ATLANTA J.-CONST. (June 22, 2021) (reporting that the plaintiffs allege that the company failed to protect its pipelines).

379. *See* Alex Younger, Opinion, *Ransomware Attacks Must Be Stopped—Here's How*, FIN. TIMES (June 11, 2021), https://www.ft.com/content/8a26196c-ee82-45ad-a138-16d0884f4f09 (discussing the moral hazard risk).

their cyber insurance companies have a grasp on their ransomware risk.

As attacks grow in frequency and severity, critics have claimed that cyber insurance contributes to the ransomware problem by making it more likely that victims can fund ransoms.[380] In thinking about how cyber insurance is shaping ransomware, some argue that coverage enables victims to pay, and payment demonstrates ransomware profitability, which increases the likelihood of future, increased ransoms.[381] According to one study, "a victim paying the ransom demand imposes a negative externality on peers who now face a higher threat level; victims are more likely to pay if insurers indemnify some or all of the payment."[382] Of course, this assumes that the carrier agrees to pay the claim.

Some regulators are attempting to deter insurance companies from paying policyholders who suffer a ransomware attack. There are restrictions on such payments being considered in Australia[383] and the United Kingdom, where a 2015

But see Katherine Chiglinsky & Jamie Tarabay, *Pipeline Attack Stirs Debate on Whether Insurance Lures Hackers,* BLOOMBERG (May 14, 2021, 6:16 PM), https://www.bloomberg.com/news/articles/2021-05-14/pipeline-attack-stirs-debate-on-whether-insurance-lures-hackers (reporting that some argue that system vulnerabilities drive attacks).

380. *See, e.g.*, Dan Sabbagh, *Insurers 'Funding Organized Crime' by Paying Ransomware Claims,* GUARDIAN (Jan. 24, 2021), https://www.theguardian.com/technology/2021/jan/24/insurers-funding-organised-by-paying-ransomware-claims ("Insurers are inadvertently funding organised crime by paying out claims from companies who have paid ransoms to regain access to data and systems after a hacking attack, Britain's former top cybersecurity official has warned."); Younger, *supra* note 379 (suggesting hackers calibrate their demands to the victim's insurance coverage).

381. *See* Daniel W. Woods & Rainer Böhme, How Cyber Insurance Shapes Incident Response: A Mixed Methods Study (unpublished manuscript) (presented at 20th Annual Workshop on the Economics of Information Security (WEIS 2021)) at 21–22 (June 7, 2021), https://informationsecurity.uibk.ac.at/pdfs/DW2021_HowInsuranceShapes_WEIS.pdf (discussing "ransom inflation").

382. *Id.* (also noting that market concentration in physical kidnap insurance enables the negotiation standards necessary to prevent ransom inflation and improves negotiations).

383. *See, e.g.*, *Locked Out: Tackling Australia's Ransomware Threat*, DEP'T OF HOME AFFS.: CYBER SECURITY INDUSTRY ADVISORY COMMITTEE (Mar. 10, 2021), https://www.homeaffairs.gov.au/cyber-security-subsite/files/tackling-ransomware-threat.pdf (noting that some ransomware payments may violate the instrument of crime provisions of the Australian criminal code); Catalin

law prohibits insurance firms from reimbursing the payment of terrorist ransoms.[384]

Insurance companies are also feeling pressure from the payment of claims. In November 2020, a German insurance company, Alliance, reported that cyber insurance claims for the previous nine months had increased 950% over the prior three years.[385] Premiums are rising; the cost of insurance rose 35% in the first quarter of 2021 and another 56% in the second quarter.[386] Cyber insurance companies are imposing lower limits in high-risk sectors such as healthcare and education.[387] In addition, exactly *what* is covered is increasingly an object of disagreement and litigation.[388] In May 2021, French insurer AXA announced that it will no longer underwrite cyber insurance policies to reimburse companies for ransom payments made to retrieve stolen or locked data, although it will continue to cover losses for responding to and recovering

---

Cimpanu, *New Australian Bill Would Force Companies to Disclose Ransomware Payments,* RECORD (June 21, 2021) https://therecord.media/new-australian-bill-would-force-companies-to-disclose-ransomware-payments/ (discussing the Ransomware Payments Bill 2021).

384. *See e.g.*, Frank Bajak, *Ransomware Gangs Get Paid Off as Officials Struggle for Fix*, ASSOCIATED PRESS (June 21, 2021), https://apnews.com/article/joe-biden-europe-government-and-politics-technology-business-3b81e8116c42439566040a052617ad55. BAE Systems' threat intelligence chief claimed, "Ultimately, the terrorists stopped kidnapping people because they realized that they weren't going to get paid." *Id.*

385. Kochman, *supra* note 54 (noting 770 cyberattack claims in the first nine months of 2020, compared with 77 in all of 2016).

386. *See* Irene Madongo, *Ransomware Attacks Drive Up Cyber Insurance Prices*, LAW360 (July 27, 2021), https://www.law360.com/articles/1406913?e_id=359aee12-a668-47f6-bc99-816982fd7073&utm_source=en]gagement-alerts&utm_medium=email&utm_campaign=similar_articles (citing a report by global insurance broker Marsh); U.S. GOV'T ACCOUNTABILITY OFF., *supra* note 376, at 10 (noting that premiums rose 10-30% in late 2020).

387. U.S. GOV'T ACCOUNTABILITY OFF., *supra* note 376, at 12–13 (noting reduced coverage limits for certain sectors).

388. *See, e.g.*, G&G Oil Co. of Ind. v. Cont'l W. Ins., 165 N.E.3d 82 (Ind. 2021) (upholding insurance company's refusal to cover ransomware losses because insured's policy covered fraud but not theft); Nat'l Ink & Stitch, LLC v. State Auto Prop. & Cas. Ins., 435 F. Supp. 3d 679 (D. Md. 2020) (requiring insurer to pay insured's losses and damages resulting from decreased efficiency in protective software installed after ransom paid); New Eng. Sys., Inc. v. Citizens Ins., No 3:20-CV-017432, 2021 WL 1978691 (D. Conn. 2021) (holding that insurer acted in bad faith by misrepresenting policy provisions when it allowed the insured to make self-repairs following a cyberattack).

from ransomware attacks.[389] As mentioned with respect to the destructive NotPetya malware, litigation continues over efforts to exclude ransomware and other malware attacks from coverage using the war exclusion.[390]

2. *The Positive Potential of Cyber Insurance*

Despite the adverse selection and moral hazard risks, cyber insurance provides some relief for some ransomware victims. In addition, coverage can help prevent ransomware attacks if insurers require strong cybersecurity before they issue coverage.[391] Some cyber insurance companies already encourage policyholders to implement baseline cybersecurity practices as a standard condition to coverage.[392] In some cases, the insurance process could also provide more checkups on the preventive measures being taken by the insured,[393] although such requirements could raise the cost of insurance coverage. In the event of an attack, the cyber insurance company and its legal counsel can provide expertise and help connect the ransomware victim with digital forensics and incident response companies, along with law enforcement.

In addition, if cyber insurance were required as one of the measures[394] needed to take advantage of the safe harbor, then

---

389. D. Howard Kass, *French Insurer AXA Drops Ransomware Payment Coverage*, MANAGED SECURITY SERVICES PROVIDERS: MSSP ALERT (May 16, 2021), https://www.msspalert.com/cybersecurity-markets/europe/axa-drops-ransom-payment-coverage/.

390. *See* Santariano & Perlroth, *supra* note 323.

391. *See* Woods & Böhme, *supra* note 381, at 19–21 (discussing cyber insurance as governance).

392. Sasha Romanosky et al., *Content Analysis of Cyber Insurance Policies: How Do Carriers Price Cyber Risk?*, 5 J. CYBERSECURITY 1, 8–11 (2019) (among the cyber security questions asked by carriers, some will ask applicants about prevention measures in place). Others report that insurers are requiring better cybersecurity controls and mitigation measures, and that underwriters are requiring more detailed submissions and incorporating vulnerability scans into their decisionmaking. Shawn Rice, *Ransomware Scourge Isn't Scaring Away Cyber Insurers*, LAW360 (Aug. 13, 2021), https://www.law360.com/articles/1410736/ransomware-scourge-isn-t-scaring-away-cyber-insurers.

393. RANSOMWARE TASK FORCE, INST. FOR SEC. & TECH., *supra* note 107, at 13.

394. Insurance is regulated at the state level, so a federal requirement would require congressional authorization. The relationship between state and federal insurance regulation, however, is beyond the scope of this article.

more policies would be written and insurers could develop more accurate models for the types of coverage and the likely costs.[395] Currently, the take-up of cyber insurance is patchy, with estimates that only about 27% of companies have standalone coverage.[396] More widespread coverage would benefit the insurance market, providing more data on the costs of prevention, crisis management, and recovery, as well as data on effective security requirements.[397]

D. *Disclosure*

Use of the safe harbor could also require prompt, detailed disclosure of ransomware attacks. Most ransomware victims do not disclose the hack, which worsens the problem.[398] Prompt disclosure by ransomware victims provides law enforcement with real-time opportunities to identify and track down the cyber-attackers, and may even lead to the recovery of ransom payments.[399] As one federal official recently put it, "[I]f ransomware victims do not report these incidents, we cannot have cybersecurity, and we cannot have national security."[400]

As it stands, disclosure of a ransomware attack is only required piecemeal, and the timing and the content of disclosure are often unclear.[401] Some entities are required to dis-

---

395. *See* Andrew Granato & Andy Polacek, *The Growth and Challenges of Cyber Insurance*, 426 CHICAGO FED. LETTER (2019), https://www.chicagofed.org/publications/chicago-fed-letter/2019/426 (noting data deficiencies that challenge price modeling).

396. Martin Croucher, *Almost Half of Firms Hit by Cyberattack in 2020, Report Says*, LAW360 (Apr. 20, 2021), https://www.law360.com/articles/1376896/almost-half-of-firms-hit-by-cyberattack-in-2020-report-says (showing only a 1% increase over 2019).

397. U.S. CYBERSPACE SOLARIUM COMM'N, OFFICIAL REPORT 79–80 (2020), https://drive.google.com/file/d/1ryMCIL_dZ30QyjFqFkkf10MxIXJGT4yv/view (noting the need to identify and price risk created by cybersecurity gaps).

398. *America Under Cyber Siege: Preventing and Responding to Ransomware Attacks: Hearing Before the S. Comm. on the Judiciary*, 117th Cong. 5 (2021) (statement of Bryan A. Vorndran, Assistant Director, Cyber Division, Fed. Bureau of Investigation) [hereinafter statement of Vorndran].

399. *See* discussion *infra* Section V.F.2.

400. *See* statement of Vorndran, *supra* note 398, at 5.

401. *To Stop the Ransomware Pandemic, Start with the Basics*, ECONOMIST (June 19, 2021), https://www.economist.com/leaders/2021/06/19/to-stop-the-ransomware-pandemic-start-with-the-basics (calling U.S. requirements

close based on the sector in which they operate. Under the federal securities laws, reporting companies have to disclose the incident if it is "material."[402] Under HIPAA, as mentioned above, the attack must be disclosed if it qualifies as a "security incident."[403]

The government is currently attempting to increase reporting. Some recent requirements impose ransomware reporting obligations on pipelines,[404] and government information technology contractors.[405] The proposed Cyber Incident Notification Act of 2021 would require federal agencies, federal contractors, and critical infrastructure companies to disclose breaches of their system to the Department of Homeland Security.[406] A proposed amendment to the National Defense Authorization Act for Fiscal Year 2022 would require reporting some ransom payments to the federal government within 24 hours of payment.[407] Attorneys who practice in this area have suggested that, in order to get companies to cooperate, some

---

"vague"). Of course, many agencies include self-reporting, disclosure, and cooperation as mitigating factors in enforcement actions, but such "credit" is far from certain. *See, e.g.*, OFAC, U.S. DEP'T TREAS., UPDATED ADVISORY ON POTENTIAL SANCTIONS RISKS FOR FACILITATING RANSOMWARE PAYMENTS, *supra* note 26 (discussing mitigating factors in enforcement actions).

402. *See* Public Company Cybersecurity Disclosures, Exchange Act Release Nos. 33-10459, 34-82746, 17 C.F.R. §§ 229, 249 (Feb. 26, 2018) (suggesting that companies consider the materiality of cybersecurity risks and incidents when preparing required disclosure). In the wake of the SolarWinds Corp. cyberattack, the Securities and Exchange Commission pressed for disclosure by impacted reporting companies. *In the Matter of Certain Cybersecurity-Related Events (HO-14225) FAQs,* U.S. SEC. AND EXCH. COMM'N, https://www.sec.gov/enforce/certain-cybersecurity-related-events-faqs.

403. *See supra* note 140 and accompanying text.

404. Press Release, U.S. Dep't Homeland Sec., DHS Announces New Cybersecurity Requirements for Critical Pipeline Owners and Operators (May 27, 2021), https://www.dhs.gov/news/2021/05/27/dhs-announces-new-cybersecurity-requirements-critical-pipeline-owners-and-operators (requiring reporting to regulators and review of current practices).

405. Exec. Order No. 14,028, 86 Fed. Reg. 26 (May 12, 2021).

406. Cyber Incident Notification Act of 2021, S.2407, 117th Cong. (2021).

407. *Peters, Portman, Warner & Collins Introduce Amendment to Annual Defense Bill to Strengthen Public and Private Sector Cybersecurity,* U.S. SEN. COMM. ON HOMELAND SEC. & GOV'T AFFAIRS (Nov. 4, 2021), https://www.hsgac.senate.gov/media/majority-media/peters-portman-warner-and-collins-introduce-amendment-to-annual-defense-bill-to-strengthen-public-and-private-sector-cybersecurity (summarizing the proposed amendment including its reporting requirements).

incentives need to be offered—not just penalties for non-reporting.[408]

E. *Calibration*

Different targets need different levels of cybersecurity because ransomware attacks do more or less harm to the entity, immediate stakeholders, and society as a whole.[409] Healthcare operations may store more sensitive personal data than meat distributors. It may be more dangerous to force gas pipelines offline than small-town governments. An attack against a big company may be more extensive than an attack against a small company. Regulators have experience with calibrating levels of required compliance with the risk involved.[410]

Although compliance will be most difficult for small businesses and public institutions, those entities may need protection from ransomware attacks most of all. Small businesses are not the most publicized targets, but they are the most common.[411] Small businesses are attractive to ransomware hackers because they "typically lack the budget and resources to prevent, identify, respond to, and recover from threats."[412] A ran-

---

408. Ben Kochman, *3 Key Details To Watch As Congress Mulls Breach Report Law*, LAW360 (Nov. 24, 2021), https://www.law360.com/corporate/articles/1426996/3-key-details-to-watch-as-congress-mulls-breach-report-law?nl_pk=72e67b2b-a356-4164-9e1a-22d8437314c9&utm_source=newsletter&utm_medium=email&utm_campaign=corporate (quoting attorneys who advise breach victims).

409. *See generally* Julio Hernandez-Castro et al., *An Economic Analysis of Ransomware and Its Welfare Consequences*, ROYAL SOC'Y OPEN SCI., Mar. 2020, at 4, https://www.researchgate.net/publication/339688144_An_economic_analysis_of_ransomware_and_its_welfare_consequences (analyzing the economic differences among ransomware attacks).

410. Consider security measures at nuclear power plants, water treatment facilities, and biohazard labs.

411. *See* Amrita Khalid, *6 Things Every Small Business Needs to Know About Ransomware Attacks,* INC. MAG. (June 25, 2021), https://www.inc.com/amrita-khalid/ransomware-hackers-crime-cybersecurity-tips.html (encouraging small businesses to back up their data and secure remote workers); Thomas Koulopoulos, *60 Percent of Companies Fail in 6 Months Because of This (It's Not What You Think),* INC. MAG. (May 11, 2017), https://www.inc.com/thomas-koulopoulos/the-biggest-risk-to-your-business-cant-be-eliminated-heres-how-you-can-survive-i.html (noting that more than 70% of attacks target small businesses).

412. *See* Khalid, *supra* note 411.

somware attack may force a small business to close its doors.[413] The threat of federal prosecution of those businesses, and those who assist them in payment of a ransom, may only worsen the situation.

F. *A Safe Harbor May Help Victims, Regulators, and Law Enforcement*

1. *Helping Ransomware Victims*

The proposed safe harbor regime would not only harden potential ransomware targets, making an attack less likely, it would also help targets if an attack nonetheless occurs. A ransomware victim who has followed the safe harbor requirements would, in its discretion, be able to pay a ransom (directly or through an entity assisting it) without the threat of prosecution by the government. For example, OFAC, which would be in the loop because of the disclosure required by the system, could either issue a license or promise no action against the victim and those who assist it.[414]

An entity that successfully meets the safe harbor requirements and nevertheless suffers a ransomware attack may find that its compliance program also serves as a defense to private lawsuits. Terrorist attack victims suing under ATA/JASTA may have difficulty in collecting damages from ransomware victims who paid with the government's assistance, or at least knowledge, in compliance with best practices.

The safe harbor may also be relevant if there is uninsured fallout from the attack and the ransomware victim confronts claims by shareholders or (if it is a healthcare organization)

---

413. *See* Koulopoulos, *supra* note 411 (noting that almost 50% of small businesses have experienced a cyberattack). *See also* discussion *supra* Section III.A.

414. As required under AMLA, FinCEN issued a report in June 2021 announcing that it was going to establish a no-action letter process regarding the application of AML to specific conduct. *See* U.S. DEPT. OF TREAS. FIN. CRIMES ENF'T NETWORK, A REPORT TO CONGRESS ASSESSMENT OF NO-ACTION LETTER IN ACCORDANCE WITH SECTION 6305 OF THE ANTI-MONEY LAUNDERING ACT OF 2020 (June 28, 2021), https://www.fincen.gov/sites/default/files/shared/No-Action%20Letter%20Report%20to%20Congress%20per%20AMLA%20for%20ExecSec%20Clearance%20508.pdf. However, the conventional, lengthy, no-action letter process would be unhelpful in a ransomware context and would not limit other regulators from pursuing their own enforcement actions.

patients. The ransomware victim's fulfillment of best practice obligations, and the government's decision not to bring any charges in connection with the attack, may form the basis of a strong defense to such claims.

2. *Helping U.S. Regulators and Law Enforcement*

More information makes better rules. Understanding what entities confront when hit by a ransomware attack requires information from those entities, and their cooperation. If U.S. regulators have better information about attacks, including what worked and what did not work, they can craft more effective compliance, interdiction, and recovery regimes.

In addition, real-time cooperation and disclosure to law enforcement would facilitate efforts to shut down hackers.[415] For example, if U.S. enforcement agencies are involved from the beginning of a ransomware attack, they may be able to use the negotiations to track and stop the hackers.[416] In 2021, law enforcement obtained a decryption key that helped victims of the REvil Kaseya attack recover their data without paying a ransom.[417] Authorities and cyber-specialists also reportedly accessed REvil's computer network, forcing the group offline.[418]

Law enforcement has had some success identifying and prosecuting hackers. As noted, in 2018, the DOJ indicted three Iranians for the SamSam ransomware attacks that crippled entities worldwide, including the MedStar Health hospital system here in the United States.[419] Similarly, in December 2020, a California grand jury indicted three North Koreans for

---

415. *See* statement of Downing, *supra* note 15 (noting that reporting would provide "timely access to evidence that could prove critical to identifying and prosecuting offenders.").

416. Daniel Silver et al., *Gov't Authorities Should Assist Ransomware Targets,* LAW360 (May 21, 2021), https://www.law360.com/articles/1386039/gov-t-authorities-should-assist-ransomware-targets.

417. Joseph Menn & Christopher Beng, *EXCLUSIVE Governments Turn Tables on Ransomware Gang REvil by Pushing It Offline,* REUTERS (Oct. 21, 2021), https://www.reuters.com/technology/exclusive-governments-turn-tables-ransomware-gang-revil-by-pushing-it-offline-2021-10-21/ (noting that authorities delayed providing the key to victims in order to pursue the hackers).

418. *Id.* This effort followed an earlier shutdown of the group in July 2021. The group reportedly later restarted operations using backup servers, but some of the group's internal systems were already controlled by law enforcement.

419. *See* discussions *supra* Sections II.C.2 & III.B.3.

malware attacks between 2009 and 2020[420] that included the 2014 Sony Pictures cyberattack[421] and other ransomware.[422] In 2021, U.S. authorities indicted two persons connected with the REvil ransomware attacks, including the hacks of Kaseya in 2021 and those on Texas municipalities in 2019.[423] The United States has offered substantial rewards for information to bring ransomware groups' leadership and participants to justice.[424]

In this respect, the fact that ransomware hackers typically seek payment in cryptocurrencies may be helpful. The public nature of some online financial platforms[425] may enable blockchain tracing firms to match a pseudonym with a particu-

---

420. Indictment, United States v. Jon Chang Hyok et al., No. CR 2:20-cr-00614 (C.D. Cal. Dec. 8, 2020) [hereinafter Indictment].

421. *Id.* at ¶ 39; *see also* James Cook, *Here's Everything We Know About the Mysterious Hack of Sony Pictures*, BUS. INSIDER (Dec. 4, 2014) https://www.businessinsider.com/guardians-of-peace-hackers-sony-pictures-2014-12 (reporting that the hackers referred to the movie *The Interview* and threatened to release Sony data).

422. Indictment, *supra* note 420, at ¶ 38 (t).

423. Merrick B. Garland, Attn'y Gen., Dep't of Just., Remarks on Sodinokibi/REvil Ransomware Arrest (Nov. 8, 2021), https://www.justice.gov/opa/speech/attorney-general-merrick-b-garland-deputy-attorney-general-lisa-o-monaco-and-fbi-director (announcing the unsealing of indictments against Yaroslav Vasinskyi and Yevgeniy Polyanin).

424. *See, e.g.* Press Statement, Reward Offers for Information to DarkSide Ransomware Variant Co-Conspirators to Justice, U.S. Dep't of State (Nov. 4, 2021), https://www.state.gov/reward-offers-for-information-to-bring-darkside-ransomware-variant-co-conspirators-to-justice/ (offering up to $10 million for information leading to the identification or location of an individual holding a leadership position in the group, and up to $5 million for information leading to the arrest and/or conviction of one of the group's conspirators); Press Statement, Reward Offers for Information to Bring Sodinokibi (REvil) Ransomware Variant Co-Conspirators to Justice, U.S. Dep't of State (Nov. 8, 2021), https://www.state.gov/reward-offers-for-information-to-bring-sodinokibi-revil-ransomware-variant-co-conspirators-to-justice/ (offering up the same payment terms as the reward announced for DarkSide participants); *Maksim Viktorovich Yakubets*, U.S. DEP'T OF STATE TRANSNAT'L ORGANIZED CRIME REWARDS PROGRAM, https://www.state.gov/transnational-organized-crime-rewards-program-2/maksim-viktorovich-yakubets/ (last visited Nov. 19, 2021) (offering a reward of up to $5 million for information leading to the arrest of the Evil Corp. hacker).

425. The Bitcoin ledger, for example, is public. *See* Custers et al., *supra* note 42. However, some "anonymity enhanced currencies" are designed to make tracing transactions more difficult. *See* statement of Downing, *supra* note 15.

lar terrorist group and identify the wallet sources of particular funds and the exchanges through which they were processed.[426] Cryptocurrencies are not untraceable, and involvement from the beginning of an attack can help law enforcement and regulators uncover the identity of the recipients.

In some cases, law enforcement may even recoup the ransom paid by a ransomware victim. If law enforcement can track the payment from the initial transfer by the ransomware victim or its representative, then some of it may also be recovered.[427] In January 2021, the DOJ reportedly seized almost half a million dollars in cryptocurrency from the ransomware group NetWalker.[428] In June 2021, approximately a month after Colonial Pipeline made the $4.4 million ransom payment, the DOJ announced that $2.3 million (63.7 bitcoins) had been recovered.[429] Using the Bitcoin public ledger and a blockchain explorer, law enforcement was able to track multiple transfers of Bitcoin and, nineteen days later, to identify those that were transferred to a specific address for which the FBI had the private key.[430] In November, 2021, U.S. officials announced the

---

426. *Cryptocurrency and Other New Forms of Financial Technology: Potential Terrorist Financing Concerns and Liability*, CLEARY GOTTLIEB (June 25, 2021), https://www.clearygottlieb.com/-/media/files/alert-memos-2021/2021_06_25-terrorist-financing-concerns-and-liability-in-cryptocurrency-and-fintech-pdf.pdf (discussing possible tracing).

427. *See* Nicole Perlroth et al., *Pipeline Investigation Upends Idea That Bitcoin Is Untraceable,* N.Y. TIMES (June 9, 2021), https://www.nytimes.com/2021/06/09/technology/bitcoin-untraceable-pipeline-ransomware.html (discussing how tracing the Colonial Pipeline payment led to recovery of some of the funds).

428. *See* David Uberti, *How the FBI Got Colonial Pipeline's Ransom Money Back,* WALL ST. J. (June 11, 2021), https://www.wsj.com/articles/how-the-fbi-got-colonial-pipelines-ransom-money-back-11623403981.

429. About two weeks before the recovery was announced, DarkSide had claimed that its servers had been seized. *Id.*; *see also* Press Release, U.S. Dep't of Justice, Department of Justice Seizes $2.3 Million in Cryptocurrency Paid to the Ransomware Extortionists Darkside (June 7, 2021), https://www.justice.gov/opa/pr/department-justice-seizes-23-million-cryptocurrency-paid-ransomware-extortionists-darkside (explaining that the seized bitcoin were "proceeds traceable to a computer intrusion and property involved in money laundering").

430. Aff. in Support of an Application for a Seizure Warrant, Case 3:21-mj-70945-LB (N.D. Cal. June 7, 2021), ¶¶ 28–33, https://www.justice.gov/opa/press-release/file/1402056/download (chronicling the transfers of the Bitcoin ransom between May 8, 2021 and May 27, 2021).

recovery of $6.1 million traceable to ransom payments received by REvil hackers.[431]

Conclusion

Ransomware is a threat to the operation of our public and private institutions, and national security itself. The law must respond. The United States has recognized the importance of its digital security in many contexts and, with the explosion of ransomware attacks during the last few years, regulators need to create a plan for both public and private actors to ensure security. Simply using existing measures to threaten regulatory enforcement actions against ransomware victims and those who assist them, however, is unlikely to spur adoption of sound security measures or even to stop payments, and may be counterproductive if it leads victims to conceal attacks. A positive incentive, such as a safe harbor for ransomware payments with clear requirements, would encourage potential targets to harden their defenses. The resulting "cyber best practices" would help protect stakeholders, provide operational confidence for U.S. entities, and defend national security.

431. Merrick B. Garland, Attn'y Gen., Dep't of Just., Remarks on Sodinokibi/REvil Ransomware Arrest (Nov. 8, 2021), https://www.justice.gov/opa/speech/attorney-general-merrick-b-garland-deputy-attorney-general-lisa-o-monaco-and-fbi-director (describing the $6.1 million as "tied to the ransom proceeds of [an] alleged REvil ransomware attacker").