ReedSmith

Driving progress
through partnership

# Is Paying a Ransom to Stop a Ransomware Attack Illegal?

Authors: Bart W. Huffman, Michael J. Lowell, Wendell J. Bartnick, Julianne K. Nowicki

Cyber extortion has become an attack of choice for some hackers. Hackers have found that extorting organizations may be a better business model than stealing data and trying to sell it on the black market. As more data breaches occur, the value of such data on the black market falls. One type of cyber extortion is ransomware. Ransomware is a form of malware that encrypts data where an organization stores it, and only the attacker has the key to decrypt it. With this attack, an organization still possesses the data; however, the organization is very unlikely to be able to decrypt the data without the hacker's key. So the encrypted data is unusable to the organization without that key. The hacker contacts the organization asking for payment in exchange for the decryption key. If the organization refuses to pay, the data remains encrypted and unusable. If the organization pays, the attacker may provide the decryption key so the organization can recover the data. The sophistication of the malware (and the ransom amounts) has grown tremendously over the past couple of years.

When victimized by a ransomware attack, organizations are faced with many difficult questions, including whether or not to actually pay the ransom. One consideration for answering that question is whether an organization is permitted to pay a ransom under U.S. law.

**U.S. Law Generally Does Not Prohibit Paying a Ransom for the Return of People or Goods.** U.S. law criminalizes receiving, possessing, or disposing of money that at any time has been delivered as ransom for a kidnapping.[1] There is no generally applicable law prohibiting individuals or organizations from paying ransoms for the return of individuals or goods. However, an important wrinkle to the analysis is that the U.S. government has prohibited any financial transactions (including ransom payments) with certain governments, organizations, and individuals that are on U.S. Sanctions Lists.

**Sanctions Lists.** The United States, through the U.S. Department of the Treasury's Office of Foreign Assets Control ("OFAC"), can impose sanctions on governments that sponsor terror,[2] groups that have been deemed Foreign Terrorist Organizations, individuals that have been deemed Specially Designated Nationals,[3] and persons otherwise sanctioned under a variety of statutory authorities. OFAC places these governments, groups, and individuals on sanctions lists, which include OFAC's Specially Designated Nationals List ("SDN" List) and Sectoral Sanctions Identifications List ("SSI") and a variety of other lists of prohibited, debarred, or otherwise restricted or sanctioned parties generally available on the U.S. Consolidated List.[4] The U.S. Consolidated List is a comprehensive watchlist that screens the SDN and SSI Lists, as well as sanctions watchlists imposed by the U.S. Department of State, Directorate of Defense Trade Controls ("DDTC") and U.S. Department of Commerce, Bureau of Industry and Security ("BIS"). The U.S. government's power to sanction arises from the Immigration and Nationality Act,[5] the National Emergencies Act,[6] the International Emergency Economic Powers Act,[7] and other treaties and laws.

---

[1] *See* 18 U.S.C. § 1202 ("Whoever receives, possesses, or disposes of any money or other property, or any portion thereof, which has at any time been delivered as ransom or reward in connection with a violation of section 1201 of this title, knowing the same to be money or property which has been at any time delivered as such ransom or reward, shall be fined under this title or imprisoned not more than ten years, or both.").
[2] *See* U.S. DEPARTMENT OF STATE, COUNTRY REPORTS ON TERRORISM 2015: STATE SPONSORS OF TERRORISM, https://www.state.gov/j/ct/rls/crt/2015/257520.htm.
[3] *See* 8 U.S.C. § 1189,.
[4] *See* U.S. DEPARTMENT OF THE TREASURY, OFFICE OF FOREIGN ASSETS CONTROL – SANCTIONS PROGRAMS AND INFORMATION, https://www.treasury.gov/resource-center/sanctions/Pages/default.aspx.
[5] 8 U.S.C. § 1189.
[6] 50 U.S.C. § 1601 et seq.
[7] 50 U.S.C. 1705.

Sanctions watchlists are also maintained under international sanctions regimes. For example, the European Union ("EU") administers the EU Consolidated Screening List, which lists persons, groups, and entities subject to the EU's financial sanctions in addition to lists that may be maintained by the Member States.[8] Similarly, the United Nations ("UN") administers the Consolidated UN Security Council Sanctions List, which lists individuals and entities subject to sanctions imposed by the UN Security Council.[9] For the purpose of this paper, "Sanctions Lists" means any and all of these various sanctions lists.

**Sanctions Lists May Include Hackers, Hacker Groups, and Governments Known To Support Hackers.** Illegal cyber activities (e.g., hacking) have been declared a national emergency and can result in the actors being added to the Sanctions Lists.[10] For example, OFAC imposed sanctions on two Russian individuals for engaging in malicious cyber-enabled activities.[11] One of the individuals was responsible for the development and use of Cryptolocker, a form of ransomware, which infected over 120,000 U.S. victims. According to OFAC, he and his group are responsible for taking over $100 million from financial institutions and government agencies. Therefore, organizations are on notice that ransom requests may be made by governments, groups, and individuals that are on the Sanctions Lists precisely because they have previously initiated ransomware attacks.

**Consequences of Being on Sanctions Lists.** Typical economic sanctions for governments, groups, and individuals on Sanctions Lists include freezing assets in the United States and blocking all financial transactions with U.S. persons: "Any property or interests in property of the [individuals or entities on the Sanctions Lists] within U.S. jurisdiction must be blocked and U.S. persons are generally prohibited from engaging in transactions with them."[12] U.S. persons may not engage in dealings with individuals or entities listed on OFAC's SDN List. OFAC's 50% Rule also prohibits U.S. persons from dealing with entities that are directly or indirectly owned 50 percent or more in the aggregate by SDNs.[13]

**Trading with the Enemy.** Pursuant to the Trading with the Enemy Act, the United States may prosecute individuals and organizations that "have materially assisted, sponsored, or provided financial, material, or technological support for, or goods or services in support of, any activity [of an individual or entity on the Sanctions Lists] or any person whose property and interests are blocked."[14] Unless otherwise authorized or exempt, transactions by U.S. persons or organizations are considered "material support" and are prohibited if they involve transferring, paying, exporting, withdrawing, or otherwise dealing in the property or interests in property of an entity or individual listed on the Sanctions Lists.[15]

OFAC has stressed that it has never given "authorization" for any ransom payments and supports a no-ransoms policy for various policy reasons.[16] Even though the United States government's policy is to not pay ransom to kidnappers, and a ransom payment may be prohibited by law in some cases (e.g., a payment to an organization on Sanctions Lists), former President Obama issued a policy directive which noted, in part, "that no family of an American hostage has ever been prosecuted for paying a ransom for

---

[8] *See* European Union External Action, *Consolidated List of Sanctions* (Aug. 18, 2015), https://eeas.europa.eu/headquarters/headquarters-homepage_en/8442/Consolidated%20list%20of%20sanctions.

[9] *See* UNITED NATIONS SECURITY COUNCIL SUBSIDIARY ORGANS, CONSOLIDATED UNITED NATIONS SECURITY COUNCIL SANCTIONS LIST, https://www.un.org/sc/suborg/en/sanctions/un-sc-consolidated-list.

[10] *See* 31 C.F.R. Part 578, Executive Order 13694, 80 Fed. Reg. 18077 (Apr. 1, 2015), https://www.gpo.gov/fdsys/pkg/FR-2015-04-02/pdf/2015-07788.pdf; U.S. Department of the Treasury, *OFAR FAQs: Other Sanctions Programs*, #447, RESOURCE CENTER, https://www.treasury.gov/resource-center/faqs/Sanctions/Pages/faq_other.aspx#cyber.

[11] *See* Press Release, *Treasury Sanctions Two Individuals for Malicious Cyber-Enabled Activities* (Dec. 29, 2016), https://www.treasury.gov/press-center/press-releases/Pages/jl0693.aspx.

[12] *See id.*; Trading with the Enemy Act, ch. 106, 40 Stat. 411 (1917), https://www.gpo.gov/fdsys/pkg/USCODE-2011-title50/html/USCODE-2011-title50-app-tradingwi-other.htm.

[13] *See* U.S. Department of the Treasury, *Revised Guidance on Entities Owned by Persons Whose Property and Interests in Property Are Blocked*, RESOURCE CENTER (Aug. 13, 2014), https://www.treasury.gov/resource-center/faqs/Sanctions/Pages/faq_general.aspx#50_percent.

[14] *See* 31 C.F.R. Part 578, Executive Order 13694, 80 Fed. Reg. 18077 (Apr. 1, 2015), https://www.gpo.gov/fdsys/pkg/FR-2015-04-02/pdf/2015-07788.pdf.

[15] *See* 18 U.S.C. 2339B; U.S. DEPARTMENT OF THE TREASURY, OFAC OFFICE OF FOREIGN ASSETS CONTROL: CYBER-RELATED SANCTIONS PROGRAM (2017), https://www.treasury.gov/resource-center/sanctions/Programs/Documents/cyber.pdf

[16] *See e.g.*, Press Release, *Remarks of Under Secretary for Terrorism and Financial Intelligence David S. Cohen at The Carnegie Endowment For International Peace, "Attacking ISIL's Financial Foundation"* (Oct. 23, 2014), https://www.treasury.gov/press-center/press-releases/Pages/jl2672.aspx.

the return of their loved ones."[17] It is less clear whether the U.S. government would take a lenient approach in the context of a ransom for the return of data or other commercial interests and unclear how the current administration views these issues.

**Possible Penalties.** The potential penalties vary depending on the statutory authority for the sanction but generally include the risk of significant monetary penalties and criminal penalties, which may include fines and imprisonment. However, we are not aware of any prior convictions or civil penalty settlements on the basis of a payment of ransom to a sanctioned party.

**Implications.** The payment of a ransom may implicate a number of legal risks that must be carefully considered alongside the inherent commercial and cybersecurity risks. As described in this paper, one such risk is the requirements of complying with sanctions, which may be relevant to the legality of the payment, the possible avenues for making payment, and the U.S. government's expectations for potential ransom payors. Organizations subject to a ransomware attack should consult experienced legal counsel to navigate these issues.

[17] *See* The White House, Office of the Press Secretary, *Statement by the President on the U.S. Government's Hostage Policy* (Jun. 24, 2015), https://obamawhitehouse.archives.gov/the-press-office/2015/06/24/statement-president-us-governments-hostage-policy-review.