Harvard Law School Forum on Corporate Governance

A Guide for Boards and Companies Facing Ransomware Demands

Posted by Antonia M. Apps, Adam Fee, and Matthew Laroche, Milbank LLP, on Saturday, October 16, 2021

Editor's note: Antonia M. Apps and Adam Fee are partners and Matthew Laroche is special counsel at Milbank LLP. This post is based on their Milbank memorandum.

On September 21, 2021, the U.S. Department of the Treasury announced a set of actions designed to counter ransomware, principally by discouraging ransomware payments. The Department of the Treasury's Office of Foreign Assets Control's ("OFAC") for the first time designated a virtual currency exchange for facilitating financial transactions for ransomware actors. OFAC also issued an updated advisory about ransomware that, among other things, emphasized that the U.S. government continues to strongly discourage ransomware payments and strongly encourage reporting to and cooperating with government agencies in the event of an attack.[1]

Though the Department of the Treasury's actions do not prohibit victim companies from paying ransoms, they add another layer of complexity for victim companies deciding whether to pay. Paying a ransom carries short-term and long-term consequences, carries legal and regulatory risk, as highlighted by the Department of the Treasury's recent actions, and could shape the outlook and reputation of a company for years to come. The decision also is one most companies will have to make. Ransomware groups continue to proliferate, and attacks have become more common, sophisticated, and successful. In addition to the Department of the Treasury, several other law enforcement and regulatory bodies have issued guidance and made public statements discouraging ransomware payments and describing the risks from making them. Among other things, they note that paying the ransom encourages future attacks against the victim company and others, and does not guarantee the restoration of data or the return of stolen data without public disclosure.[2]

---

[1] *See* Press Release, U.S. Dep't of the Treasury, Treasury Takes Robust Actions to Counter Ransomware (Sept. 21, 2021), *available at* https://home.treasury.gov/news/press-releases/jy0364; Updated Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments, U.S. Dep't of the Treasury (Sept. 21, 2021), *available at* https://home.treasury.gov/system/files/126/ofac_ransomware_advisory.pdf (the "OFAC Advisory").

[2] Cybersecurity and Infrastructure Security Agency ("CISA"), Ransomware: What It Is and What to Do About it (2020), *available at* https://us-cert.cisa.gov/sites/default/files/publications/Ransomware_Executive_One-Pager_and_Technical_Document-FINAL.pdf; FBI, Ransomware Prevention and Response for CISOs, *available at* https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view; FinCEN, Advisory on Ransomware and the Use of the Financial System to Facilitate Ransom Payments (Oct. 1, 2020), *available at* https://www.fincen.gov/sites/default/files/advisory/2020-10-01/Advisory%20Ransomware%20FINAL%20508.pdf (the "FinCEN Advisory"); N.Y.S. Dep't of Fin. Servs., Insurance Circular Letter No. 2, Cyber Insurance Risk Framework (2021), *available at* https://www.dfs.ny.gov/industry_guidance/circular_letters/cl2021_02#_ednref11 ("NYDFS Guidance"); *see also* Video, Senate Judiciary Committee Holds a Hearing On Responding to Ransomware Attacks, YouTube (July 27, 2021), *available at* https://www.youtube.com/watch?v=MQNwFKyt3fI ("Senate Judiciary Video") (FBI Assistant Director of Cyber Division reporting that the FBI is currently tracking approximately 100 different ransomware variants or groups).

While those concerns are all valid, the practical reality is that paying a ransom may make the difference between the failure or survival of a business. Victim companies and the boards overseeing them must be prepared to decide whether to pay quickly, pragmatically, and decisively. We previously wrote about modern ransomware variants and the steps a company should take immediately following an attack to contain the incident, resume normal business operations, and appropriately assess legal and regulatory risks. *See* Antonia Apps, Adam Fee, & Matthew Laroche, *What Companies Need to Know About Modern Ransomware Attacks and How to Respond*, Harv. L. Sch. Forum on Corp. Governance (July 14, 2021), *available here*. Below we address specifically the legality of paying the ransom and the potential applicability of the U.S. sanctions regime and anti-money laundering statutes, particularly in light of recent actions by the Department of the Treasury. After exploring the legal considerations, we recommend three practical assessments for companies determining whether to pay, including valuing the breached data in the context of a modern ransomware attack, the practical risks from paying the ransom, and methods for negotiating and paying. While every company and attack is unique, these assessments will help prepare companies deciding whether to pay.

Paying the Ransom is Not Illegal Per Se, But Companies Need to Mitigate Risks Associated with Sanctions and Anti-Money Laundering Laws

There is no existing law in the United States that prohibits a company from paying a ransomware ransom. While several states—New York, North Carolina, and Pennsylvania—are considering legislation that would ban state and local government agencies from paying such a ransom, as of this publication, that legislation has not passed. Nevertheless, OFAC's recent advisory highlights the risks of sanctions enforcement from paying a ransomware criminal.

The OFAC Advisory, which updates similar OFAC guidance issued on October 1, 2020, stressed the national security risks posed by ransomware payments, and stated that those who facilitate such payments may run afoul of the U.S. sanctions regime. U.S. sanctions are enforced by OFAC and the Department of Justice ("DOJ") under the authority of the International Emergency Economic Powers Act ("IEEPA"), the Trading with the Enemy Act ("TWEA"), and various Executive Orders and regulations. Under that regime, U.S. persons, which include companies operating under the laws of the United States, are generally prohibited from engaging in financial transactions, directly or indirectly, with individuals or entities on OFAC's Specially Designated Nationals and Blocked Persons List ("SDN List"), other sanctioned entities, and those covered by comprehensive country or region embargoes (*e.g.*, North Korea and Syria). The OFAC Advisory makes clear that many ransomware criminals are designated pursuant to its cyber-related sanctions program. Furthermore, both U.S. and non-U.S. persons are prohibited from causing a U.S. person to violate any sanctions, such as by causing a U.S.-based bank to pay a sanctioned entity. OFAC may impose civil penalties for sanctions violations based on strict liability, such that a company may be subject to civil liability even where it did not know or have reason to know, it was engaging in a prohibited transaction.

On October 1, 2020, the U.S. Financial Crimes Enforcement Network ("FinCEN") issued a similar advisory directed toward financial institutions that might process ransomware payments. *See supra* note 2, the FinCEN Advisory. Under anti-money laundering laws, financial institutions generally must seek to identify and report suspicious activity. Ransomware criminals are increasingly using cryptocurrency to facilitate ransomware payments, and financial institutions could be liable where they fail to identify and report those payments. Shortly after FinCEN's

advisory, the DOJ released its "Cryptocurrency Enforcement Framework" report, discussing the risks and enforcement initiatives related to cryptocurrency-related crime, including ransomware. *See* Dep't of Justice, Report of the Attorney General's Cyber Digital Task Force, Cryptocurrency Enforcement Framework (Oct. 2020), *available here*. That report discusses the various law enforcement and regulatory bodies that might be implicated by a ransomware payment using cryptocurrency, including in addition to DOJ, OFAC, and FinCEN, the Securities and Exchange Commission, the Office of the Comptroller of the Currency, the Commodity Futures Trading Commission, the Internal Revenue Service, and state and international authorities.

Beyond the sanctions regime and anti-money laundering laws, other laws are theoretically implicated by paying a ransomware criminal. For example, it is illegal to provide material support to a foreign terrorist organization, including by paying such an organization large sums of money, *see* 18 U.S.C. § 2339B; to conspire with others to hack a computer system and extort the victim, *see* 18 U.S.C. § 1030(a)(7); or to bribe foreign officials or entities in exchange for obtaining or retaining business in that country, 18 U.S.C. § 78dd-1. Although it seems unlikely, and legally dubious, for law enforcement to pursue a victim company for potentially violating one of those statutes for making a ransom payment, every situation is unique and must be assessed individually.

In positive news for victim companies, we are not aware of a victim company being targeted by law enforcement for paying a ransomware criminal. This makes sense. Bringing such a case would discourage victims from cooperating with law enforcement at a time when officials are imploring victim companies to work with them following an attack. The OFAC Advisory "strongly encourages" all victims to cooperate with federal law enforcement following an attack and report any ransomware payments to Treasury's Office of Cybersecurity and Critical Infrastructure Protection ("OCCIP") and OFAC, if there is reason to suspect a potential sanctions nexus. Moreover, on July 27, 2021, several top federal law enforcement officials, including the Assistant Director of the FBI's Cyber Division and Assistant Director of the Secret Service's Office of Investigations, encouraged Congress *not* to ban ransomware payments because, among other reasons, it would discourage victims from cooperating with law enforcement. *See* Dep't of Justice, Statement of Bryan A. Vorndran Before the Committee on the Judicary, U.S. Senate (July 27, 2021), *available here*; *see also* Video, Senate Judiciary Committee Holds a Hearing On Responding to Ransomware Attacks at 1:20.00, YouTube (July 27, 2021), *available here*.

Charging victim companies also would be inconsistent with the federal government's traditional policy not to prosecute victims for paying ransoms in hostage situations, even if those payments are made to foreign terrorist organizations or other sanctioned entities or individuals. *See* Press Release, The White House, Statement by the President on the U.S. Government's Hostage Policy Review (June 24, 2015), *available here*. There also are a variety of other practical and legal reasons why it would be difficult to charge a victim company. For example, a significant problem in bringing a sanctions case following a ransomware payment is establishing which cybercriminal was responsible for the attack in question. The FBI has acknowledged that attribution following ransomware attacks is "extremely challenging" and that in about half of cases, the FBI is unable to determine who committed the hack. *See supra* note 2, Senate Judiciary Video.

While civil or criminal exposure from the government has not yet followed because a victim company paid a ransom, the foregoing discussion highlights the need for companies to mitigate the risk of an enforcement action following an attack. In addition to consulting with experienced counsel, companies also should ensure they have an appropriate sanctions compliance program and consider contacting law enforcement and/or OFAC following an attack, which are significant mitigating considerations in OFAC's enforcement determinations. *See supra* note 1, OFAC Advisory (stating that "a significant mitigating factor" in evaluating an enforcement action is a "self-initiated and complete report of a ransomware attack to law enforcement or other relevant U.S. government agencies," including OFAC).

Practical Considerations for Paying the Ransom

The fact that paying the ransom is not illegal in and of itself does not make deciding whether to pay any less difficult. Planning how to make that decision is key. Companies and their boards that have methodically pre-identified important factors in paying the ransom will be prepared to pragmatically and decisively address the problem when it arises. We recommend three assessments for victim companies deciding whether to pay: (i) the value of the breached data in light of modern ransomware attacks; (ii) the risks from paying the ransom; and (iii) negotiation and payment options.

Valuing the Breached Data

The value of the breached data is in many circumstances the overriding consideration for victim companies. In the most extreme cases, such as where hackers have shut down a computer network necessary for public safety, the choice might be simple—the victim company will pay to try to save lives. In most attacks, however, the decision is not as stark and companies will have to carefully consider the value of their data in the context of modern ransomware attacks. There are several aspects to this assessment:

Uninfected Backup Data and Ability to Rebuild the Network: Victim companies should first consider whether the breached data is unnecessary to business operations, backed up on an uninfected system, and/or the network can be rebuilt without unnecessary disruption to business activities. Any of those circumstances presents the ideal post-breach scenario because there would be no reason to pay the ransomware criminal. Unfortunately, modern ransomware attacks have complicated matters and make those scenarios less likely. As we have written about previously, modern attacks are highly sophisticated with ransomware criminals infiltrating networks for weeks or months so that they can move laterally to gain access to more parts of the network, identify the most sensitive data stored by the victim, and infiltrate backups making it harder for victims to recover from an attack. As a result, victim companies have difficulty assessing the duration and scope of the breach, which makes it harder for the victim company to determine the extent of the breached data or whether it can fully rebuild based on uninfected backups. Relatedly, because attacks are targeting companies' most sensitive data in an effort to inflict immense damage for higher payouts, it is becoming more likely that the breached data is crucial to business operations.

Leverage Public Sources: Even where companies determine that the breached data is critical, paying the ransom still may be unnecessary. There are publicly available repositories of keys and applications that can decrypt data locked by different types of ransomware variants. For example,

the National High Tech Crime Unit of the Netherlands' police, Europol's European Cybercrime Centre, and several cyber security companies have created a database of decryption tools for more than 85 different types of ransomware variants. *See* No More Ransom Portal, *available here*. The FBI and CISA also have access to a variety of decryption tools, and may have other ways to pressure cybercriminals for decryption keys, including engaging foreign counterparts in countries where the hackers are operating. Victim companies should assess whether any of these available resources can resolve the breach and decrypt the data without engaging the cybercriminal.

The Impact from Public Disclosure of Data: Modern ransomware attacks often involve "double extortion" in which the ransomware not only encrypts the victim's data, but also exfiltrates it from the victim's network. In those circumstances, the existence of uninfected backup files or a public decryption key might be beside the point as victim companies will need to assess the damage from public disclosure of their data. That assessment will involve various business considerations, such as potential reputational harm and client/customer relationships.

There are additional legal considerations as well, including an assessment of potential claims against the company by customers and/or consumers whose data was breached, or regulatory bodies overseeing the victim company. Where consumer data is involved, private rights of action under state consumer protection laws have led to class action litigation, as well as related claims of negligence, breach of fiduciary duty, and breach of contract. *See, e.g.*, *In Re Blackbaud, Inc., Customer Data Breach Litig.*, No. 20 Civ. 2972 (JMC), 2021 WL 2718439, at *2 (D.S.C. July 1, 2021); *Stoll v. Musculoskeletal Inst., Chartered*, No. 20 Civ. 1798 (AAS), 2020 WL 6784115, at *1 (M.D. Fla. Nov. 18, 2020); *see also See Grifo & Co., PLLC v. Cloud X Partners Holdings, LLC*, 485 F. Supp. 3d 885 (E.D. Mich. 2020); *Surfside Non-Surgical Orthopedics P.A. v. Allscripts Healthcare Sols., Inc.*, No. 18 Civ. 566, 2019 WL 2357030, at *1 (N.D. Ill. June 4, 2019).

The Supreme Court recently issued an opinion tightening the standing requirements in data breach cases, holding that "the risk of future harm [from a data breach] on its own does not support Article III standing for the plaintiffs' damages claim." *See TransUnion LLC v. Ramirez*, 141 S. Ct. 2190, 2213 (2021). Under this rule, to establish standing, a plaintiff must show a "concrete injury" from the data breach, such as identity theft, which becomes more likely when victim data is publicly available on the Internet. Even before *Transunion*, numerous federal courts had dismissed cases where no customer data was publicly disclosed, reasoning that the victim customers did not suffer any injury and thus had no standing to assert a claim. *See, e.g.*, *See, e.g.*, *Browne v. US Fertility, LLC*, No. 21 Civ. 367, 2021 WL 2550643, at *1 (E.D. Pa. June 22, 2021); *Graham v. Universal Health Serv., Inc.*, No. 20 Civ. 5375, 2021 WL 1962865, at *1 (E.D. Pa. May 17, 2021); *Travis v. Assured Imaging LLC*, No. 20 Civ. 390 (JCH), 2021 WL 1862446, at *10 (D. Ariz. May 10, 2021); *Clemens v. ExecuPharm, Inc.*, No. 20 Civ. 3383, 2021 WL 735728, at *5 (E.D. Pa. Feb. 25, 2021); *Blahous v. Sarrell Reg'l Dental Ctr. for Pub. Health, Inc.*, No. 19 Civ. 798 (SMD), 2020 WL 4016246, at *5 (M.D. Ala. July 16, 2020) (collecting cases). Thus, victim companies are in a stronger litigation posture when the breached data is not publicly disclosed and must carefully analyze the cost of paying to prevent that disclosure versus the cost of future litigation.

Risks From Paying the Ransom

Where an assessment of the breached data suggests that payment is appropriate, companies should also consider the risks from paying (in addition to the risks of sanctions enforcement and anti-money laundering laws discussed above). In assessing those risks, it is helpful for companies to identity, potentially with the help of law enforcement and/or independent forensic investigators with ransomware expertise, the type of ransomware variant and ransomware group responsible for the attack. As we have already explained, attribution can be difficult, even for federal law enforcement officials who investigate ransomware groups for a living.

The Risk of Non-Restoration or Public Disclosure: By some estimates, one in every five companies that fall victim to an attack and pay the ransom do not receive the promised decryption key. *See* Kaspersky, *Over Half of Ransomware Victims Pay the Ransom, But Only a Quarter See Their Full Data Returned* (Mar. 30, 2021). Hackers also might simply restore victims' data a little at a time and ask for more money to recover the rest, or post the data online after payment. In at least one instance, the ransomware group Petya developed ransomware without a method to decrypt it. *See* Brian Cayanan & Anthony Melgarejo, *Petya Ransomware Attack In Progress, Hits Europe*, TrendMicro (June 27, 2017). Some ransomware variants and groups have more of a track record than others and, thus, victim companies should obtain as much information as possible when determining whether or not to pay. Of course, the fact that a ransomware group has previously upheld its promise to decrypt data or not publish data online is not a guarantee that they will do so in the future. Moreover, before paying the ransom, victim companies should consider asking for "proof of life," that is, proof that the ransomware group is capable (and willing) to decrypt the data by requiring the criminals to decrypt a test file, in order to prove that they can.

The Risk of Future Attacks: Paying the ransomware group might simply increase the likelihood that the company is attacked again in the future. In one survey, 80% of victim companies that paid a ransom reported experiencing a second attack. Of those, nearly half believed it was at the hands of the same attackers, while 34% thought the second attack was perpetrated by a different group. *See, e.g.*, Cybereason Report, Ransomware: The True Cost to Business (June 2021). Victim companies might assess that the value of their breached data far outweighs the risk of later attacks. Moreover, repeat attacks might be more a symptom of poor security practices than cybercriminals identifying a company that is willing to pay. Nevertheless, at a minimum, companies that decide to pay should be extra vigilant in identifying and fixing the breach and monitoring for additional attacks in the future.

Negotiation and Payment Options

Companies deciding whether to pay also should consider how to negotiate the ransom, payment mechanics, and whether insurance will cover some or all of the costs.

Benefits of Negotiation: In most cases, victim companies should negotiate and not simply pay the initial demand. Negotiations can give the company more time to determine whether it can decrypt the data on its own or rebuild the network through uninfected backup files. Victim companies also have had success lowering the ransom amount through negotiation. For example, in one attack, a hospital reportedly was able to negotiate a ransom down from $3.6 million to $17,000. *See* C. Everett, *Ransomware: To Pay or Not to Pay?* Computer Fraud & Security (2016). Still, in many modern ransomware attacks, criminals often explore victim

networks for weeks or even months before they emerge with ransom demands. Thus, ransomware groups often have substantial information about victims' financial health and victim companies should adjust their negotiating strategies accordingly.

Payment Mechanics: Victim companies must also have a plan in place for paying the ransom. Most ransomware groups now use cryptocurrency as their preferred method of ransom payment. Victim companies need access to cryptocurrency or a relationship with another organization that can broker payment. The failure to make good on a promise to pay can result in harsher consequences than simply refusing to pay altogether. For example, in one attack, a ransomware group reportedly posted patient health information in retaliation for the victim company failing to honor a promise to pay the ransom demand and then not responding to the ransomware group. *See Athens Orthopedic Clinic Incident Response Leaves Patients in the Dark and Out of Pocket for Protection*, Databreaches (Aug. 15, 2016).

Victim companies also should consider asking for law enforcement assistance when making a payment. For example, in the case of the May 2021 attack on Colonial Pipeline, the company paid a $4.4 million ransom in bitcoin to regain access to its systems. The FBI was involved in those negotiations and subsequently recovered a portion of the ransom by monitoring a publicly visible bitcoin ledger as hackers transferred the bitcoin ransom to other digital ledgers, which are akin to personal digital wallets. When a significant portion of the ransom, about 64 bitcoins, was transferred to a digital address for which the FBI had obtained a "private key" (*i.e.*, the password to access the address), the FBI obtained a search warrant and seized the bitcoin. *See* 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).

Insurance Coverage: Victim companies also should consider whether they have applicable insurance coverage. Cyber and related insurance policies can cover the costs of outside counsel, forensics, crisis communications, and, in some circumstances, the ransom payment. This is another area with a high potential for litigation, and some state insurance regulators have issued guidance discouraging carriers from making ransomware payments. For example, on February 4, 2021, the New York State Department of Financial Services ("NYDFS") issued a notice arguing that insurers should not make ransomware payments because they (i) could violate OFAC sanctions; (ii) might not result in the restoration of data (or return of exfiltrated data without public disclosure); and (iii) might fund future ransomware attacks against the same or other organizations. *See supra* note 2, NYDFS Guidance. Some insurers also have brought cases challenging whether a ransomware attack was covered by the insured's policy following an attack. In any event, assessing whether insurance covers some or all of the costs of an attack is important when deciding to pay or not.

* * *

Those responsible for corporate governance must be prepared to decide whether or not to pay the ransom following an attack. Though every attack and circumstance is unique, companies that make the foregoing assessments following a ransom demand will be prepared to begin the recovery process, limit legal and regulatory exposure, and determine whether to pay.