Cybersecurity Law Report cslawreport.com

Sep. 21, 2022

Ransomware

Held to Ransom: How Cyberattacks Can Become a Legal and Regulatory Odyssey for a Private Investment Fund

By
Ryan P. Blaney, Margaret A. Dale, Dorothy Murray, Todd J. Ohlms and Jonathan M. Weiss, *Proskauer*

Imagine this: you work for a private investment fund manager. It is Monday evening. The finance director of one of the fund's portfolio companies, a well-known payment services provider, calls. The company has discovered ransomware barring it from accessing the majority of its IT systems and the cyber-threat actors are demanding a ransom before they will hand over the decryption key. The ransom will double each day it remains unpaid, and if the company does not pay, the hackers will publish all of the personal information and sensitive business information they have captured. Within two days the ransom will exceed the company's cyber insurance coverage and it will need a cash injection from the investment fund to satisfy the ransom demand. What do you do?

Where business-critical information or platforms are at stake, many commercial parties will seriously consider immediately paying the ransom hoping to regain control of operations, secure client data and avoid continued business disruption and negative publicity. However, businesses may wish to pause. Determining whether to pay a ransom is not straightforward; there are inevitable legal, financial, practical and regulatory pitfalls for the unwary. Although many funds will have a written incident response plan, practiced during annual tabletop exercises, a real-life ransom attack will always create novel issues and challenges. This is because each situation is very fact specific and will be fast moving. Businesses will need to balance risks and make decisions with, at best, imperfect and, on occasions, little to no information. The steps and issues we flag in this article series may simply not be of relevance, or even possible, in any particular circumstance. Every incident may therefore prove a costly odyssey into unchartered waters.

Cyberattacks, by their very nature, know no borders and nor therefore should a private fund's response The first of this two-part series considers immediate incident response steps and analyses whether to pay a ransom, from U.S., U.K. and E.U. perspectives. The second part considers the notification obligations (to impacted individuals, regulators, investors and other stakeholders) and other consequences of a data breach of this nature in these same jurisdictions.

See "A Look Inside Businesses' Private Disputes Over Ransomware Costs" (Aug. 18, 2021).

The Cyber Landscape

U.S.

Ransomware attacks in the U.S., both by nation-states and small groups of actors, are increasing in both frequency and sophistication. Over 35 percent of global companies were estimated to be ransomware victims in 2021, and industry experts consider this estimate is low given historical under reporting of cyber incidents for fear of copycat attacks or reputational damage. In years past, most attacks involved a single extortion: attackers encrypted an organization's data and demanded a ransom in exchange for the decryption key. Today, attacks often involve exfiltrating the victim's data to an offsite location before encryption, and then threatening to leak sensitive portions of the data if the ransom is not paid. The combined threat of having your (and your clients') most sensitive data published while simultaneously being denied access to, or use of, your data has resulted in increased demands from cyber-threat actors and also complicates the legal analysis of whether the incident triggers breach notification laws in various jurisdictions.

In response to these increased threats, in February 2022, the SEC proposed new rules under the Investment Advisers Act of 1940 and the Investment Company Act of 1940 that would require registered investment advisers and funds to adopt and implement written cybersecurity policies and procedures reasonably designed to address such risks. One of the proposed rules requires advisers to report significant cybersecurity incidents affecting the adviser, or its fund or private fund clients, to the SEC, which also proposes amendments to various forms regarding the disclosure of cybersecurity risks and incidents affecting advisers, funds, their clients, and their shareholders. It subsequently announced in May the size of its Crypto Assets and Cyber Unit had nearly doubled.

See "SEC Proposes Cyber Risk Management Rules for Advisers" (Apr. 27, 2022).

U.K.

Similarly, the U.K. has seen a reported uptick in cyber-related data breaches of nearly 20% in the past two years. The Financial Conduct Authority (the U.K.'s financial services regulator) reported an increase of 50% in cyber incidents reported to it in 2021. 2022 has also seen a constant increase in the number of reported ransomware attacks in the U.K., a fact recently emphasized by the Information Commissioner's Office (the U.K.'s data protection regulator) and the National Cyber Security Centre (the U.K.'s technical authority on cyber security) in July 2022. All organizations based or operating in the U.K. are therefore coming under increased scrutiny by regulators who expect adequate measures to be in place to prevent and to respond to such attacks. Private funds are no different, and given their regulated status, and connections, through their investments, to different industry sectors, are typically subject to multiple parallel and overlapping relevant laws and regulations.

Sponsors themselves are of course a high value target in any jurisdiction, given that even relatively small sponsors often control (directly or indirectly) billions of dollars and hold highly confidential information concerning their investors and partners. Even where a portfolio company has been the subject of an attack, as opposed to the fund or the manager, monies to pay any ransom may be requested from the fund as in the scenario here, and the portfolio company and fund will each have their own considerations, whether these are regulatory, contractual or related to reputational management.

Incident Response

Given the increased focus of both U.S. and U.K. regulators on cybersecurity, funds such as the one in our hypothetical should consider practical steps to prepare and respond to a ransom attack. These will need to be assessed, of course, against the exact set of circumstances.

See "New Pressures Shift Best Practices for Ransomware Crisis Communications" (Oct. 13, 2021).

Build the Team

The right team to investigate, lead, assess risks and provide legal advice is likely to be a mix of internal experts and external advisers. Internally, IT or technical professionals along with legal and compliance will be central to the response, with support and guidance from senior leadership and management. External support and assistance can come from legal advisers, forensic providers, and public relations, threat intelligence and negotiations specialists.

Contain

At the same time as investigating (see below), the team will seek to understand whether impacted systems are isolated or whether the attack could still spread. Can the incident be contained, *e.g.*, by isolating the impacted system(s) from the network so that the threat actor cannot continue or escalate unauthorized access? The team may need to restore data from backups or rely upon other servers.

Investigate

Key items to seek to understand (to the extent possible, of course, in the available time) include:

1. the scope of data and systems are affected and to what extent;
2. whether the email systems used to manage incident response are secure and uncompromised; and
3. whether there are any clues as to the possible identity of the threat actor. Ransomware attacks can be particularly sophisticated, so the team may not be able to understand the nature and

scope of the intrusion and must make decisions with incomplete or limited information.

Consider Privilege

The process of determining how the investigation can be conducted so as to seek to protect legal privilege is beyond the scope of this article. However, there are various options such as a dual track forensic review. All parties should be aware that privilege may not necessarily apply to all communications about the incident (particularly in connection with U.K. data protection regulatory investigations, or communications to third parties). A litigation hold should also be considered.

Contact Insurers

If there is a relevant cyber policy, it will typically provide that insurers must be notified in accordance with its terms and may direct the appointment of advisers. Where there may be a conflict between insurer and policyholder (for example, a ransom demand is near or over the limit of a cyber policy), a policyholder may wish to have its own counsel as co-advisers, or at least ready in the wings. Importantly, many insurance policies contain exclusions with respect to certain cybersecurity events. Lloyds of London, for example, recently announced that, commencing in 2023, its policies would exclude coverage for cybersecurity events (including ransomware) caused by state-sponsored actors.

Notifications

There may also be notifications to regulators and/or affected individuals and/or other bodies to consider. We will consider these further in part two of this series.

Responding to Ransom Demands

Armed with the best possible understanding of the situation in the available time, if the compromised systems or data cannot easily or completely be recovered, the team will be stuck between Scylla and Charybdis. Does the company pay a ransom, potentially assuming legal and reputational risks in return for a *possible* recovery of data and systems, or does it give up on any swift attempt at recovery and suffer potentially significant business losses by refusing to give in to ransom demands?

There are two key questions to ask: *Can* the fund legally pay a ransom? If it can, *should* it pay a ransom?

See “How Law Firms Can Prevent, Detect, and Respond to Ransomware Attacks” (May 12, 2021).

1. Is It Legal to Pay a Ransom?

There is no express prohibition under U.S. or English law on paying a ransom per se, but payment could be a criminal offence in several circumstances, including if paid in breach of applicable sanctions, terrorist financing or money laundering laws.

See "To Pay or Not to Pay? Empirical Studies Show Keys to Ransomware Decisions" (Dec. 15, 2021).

Sanctions

Businesses subject to a ransomware attack will seek to consider the potential legal exposure under all applicable domestic and international sanctions regimes before making any payment.

In addition to increased attention from the SEC described above, the U.S. Treasury Department's Office of Foreign Assets Control (OFAC) issued an advisory in October 2020 declaring that any payment made to a sanctioned entity on OFAC's list would be a violation of federal sanctions regulations and the paying entity would be strictly liable. In other words, the intent of the victim, and the knowledge as to whether the entity is on OFAC's list, is no defense. While OFAC continues to highlight the heightened sanctions risk from ransomware attacks in subsequent advisories, the nature of ransomware makes it difficult for the victim of an attack to be able to identify the entity that is actually being paid. This ambiguity may cause victims of ransomware attacks to unintentionally violate OFAC's sanctions. Mitigating and aggravating factors, including potentially the extent of due diligence done, may however be taken into account in OFAC's decision whether or not to charge a paying party.

E.U. sanctions (which apply to all E.U. nationals and businesses along with any businesses who carry out activities in the E.U.) prohibit E.U. persons and businesses from making funds available to sanctioned persons and/or entities. The E.U. maintains a full list of sanctioned persons and entities and in 2019 introduced the European Sanction List for Cybercriminals, which contains specific details about sanctioned persons/entities who are known cybercriminal persons and organizations. Typically anonymous and shadowy figures, cyber-threat actors will likely provide difficult subjects for effective due diligence. A business subject to such any attack will wish to show it has taken all reasonable steps to diligence both the nature of the attack and the perpetrator to ensure – so far as possible – that the perpetrator is not a sanctioned person or entity.

All individuals and legal entities with a "U.K. nexus" must also comply with U.K. financial sanctions. This means that all acts in the U.K. or by U.K. funds or U.K. portfolio companies anywhere else in the world are within scope. The U.K.'s Office of Sanctions Implementation publishes lists of sanctioned entities. This list is similar to the E.U.'s sanctions list but not identical. Similar to the E.U. position, it is an offense in the U.K. to make funds available directly or indirectly (*i.e.* where a payment is made to a third party acting on behalf or at the direction of a sanctioned person) to a U.K.-sanctioned person or entity, unless it can be established that the payee did not know or have reasonable cause to suspect that funds would be made (in)directly available to a sanctioned person/entity. (This contrasts with the U.S. sanctions regime which, as explained, imposes strict liability.)

Businesses operating in both the E.U. and U.K. should therefore review both sets of sanction lists and undertake all reasonable diligence to ensure any ransomware payment is not subject to the re-

spective sanctions.

Under all domestic and international sanctions regimes, not only can the company be subject to significant fines, but individuals can also face fines and potential criminal prosecutions (including prison sentences). Lists of sanctioned parties change regularly in all jurisdictions and should be kept under constant review.

See "Steps to Take After OFAC and FinCEN's Warnings on Ransomware Payoffs" (Oct. 21, 2020).

Terrorist Financing

The U.K. has a specific offense to prevent terrorist financing. Similar to the U.K.'s sanctions regime, a company must not pay money if it knows or has reasonable grounds to suspect that it will or might be used for the purposes of terrorism. As such, before making any payment, and recognizing the challenges arising from the typical anonymity of perpetrators, payer must again seek to conduct reasonable due diligence to understand the identity of the payee.

The U.S. does not have a directly equivalent offense. Counter terrorist financing is one of the goals of anti-money laundering and sanctions legislation, and payment of funds to, or for use by, a terrorist organization could amount to one of more different crimes or regulatory breaches.

Money Laundering

Finally, the fund and its investee company must not assist money laundering in any relevant jurisdiction. As anti-money laundering regimes often involve a notification element, as well as requirements as to systems and controls, we will address such regimes in part two.

We will address additional notification obligations in part two.

Contractual Prohibitions

A fund may also be prohibited from making a ransom payment by the terms of its limited partnership agreement with investors or by the terms of investor side letters. Express prohibitions on paying ransoms are not yet common in the U.S. or U.K. market (although cyber security is increasing in prominence in investor negotiations), and the matter is typically viewed as one of operational fund management, in which the general partner, the manager and advisers must act in accordance with their usual fiduciary duties and duties of care. Side letters are, however, likely to prohibit payments in breach of all relevant sanctions and prevention of terrorist financing regimes, so this analysis is doubly important.

Relevant restrictions may also be found in finance documents at the fund or operating company level. Fund finance documents in particular tend to vary widely regarding prohibitions on payments to restricted persons or in breach of sanctions or anti-money laundering laws. They capture the direct and indirect use of facility proceeds as well as compliance not just by the fund but by its investment holdings companies and portfolio companies.

2. Should the Victim Pay the Ransom?

Whether an organization should pay ransom is a complex question. On the one hand, U.S. and U.K. law enforcement authorities (such as the FBI and state attorneys general in the U.S., and the U.K.'s National Crime Agency (NCA)) generally discourage organizations from paying ransoms: organizations that do, they argue, effectively reward criminals, are not guaranteed to recover the affected data or systems, and potentially make themselves "soft" targets for future cyberattacks.

On the other hand, many businesses eager to quickly recover from ransomware incidents severely impacting their businesses may be open to such payments. Similarly, many cyber insurers consider ransom payments to be a more economical alternative to covering other alternatives (such as a full-fledged systems rebuild). Importantly, however, neither the FBI nor the NCA prevent – or have prosecuted (to our knowledge) – organizations that have paid ransom provided that such payments do not violate applicable sanctions, terrorist financing or anti-money laundering laws.

See the Cybersecurity Law Report's two-part interview with the Ransomware Task Force co-leader: "Task Force Leader Discusses How to Beat Ransomware in a Year" (May 19, 2021); and "Task Force Leader Addresses Proposed Mandatory Reporting of Ransomware Payments" (May 26, 2021).

Ryan P. Blaney is the head of Proskauer's global privacy and cybersecurity group and a partner based in the firm's Washington, D.C. office.

Margaret A. Dale is vice-chair of Proskauer's litigation department and co-head of its data privacy and cybersecurity litigation practice. She is based in the firm's New York office.

Dorothy Murray is a partner in Proskauer's litigation department and a co-head of the asset management litigation group. She is based in the firm's London office.

Todd J. Ohlms is a partner in Proskauer's litigation department and a member of the asset management litigation group. He is based in the firm's Chicago office.

Jonathan M. Weiss a partner in the litigation department and co-head of the asset management litigation group at Proskauer. He is based in the firm's Los Angeles office.

Proskauer partners Seetha Ramachandran and Vishnu Shankar and special international labor, employment and data protection counsel Kelly McMullon contributed to this article.