Cybersecurity Law Report cslawreport.com

Oct. 19, 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 attackers 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?

Part one of this series set out the issues to keep in mind in terms of immediate incident response and weighing whether to pay the ransom. This second installment reviews the regulatory obligations that arise on any data breach and considers the follow-on steps and consequences of such a breach from both a U.S. and U.K. perspective.

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

Notification Obligations to Financial Markets Regulators

A fund must comply with all its regulatory duties in the event of a breach of the fund's computer systems. The regulatory notification and reports may need to be made by the fund itself, the fund's third-party vendors, the fund's portfolio companies, or a combination of these entities.

U.S.

In the U.S., the fund, as part of the financial sector, is subject to a complex set of regulations and privacy laws that apply to varying degrees depending upon the type of personal information that

the fund collects and how the fund received, used and disclosed any personal information. Some of the U.S. federal laws that include privacy and data protection requirements include the Fair Credit Reporting Act of 1970 (FCRA), the Fair and Accurate Credit Transactions Act of 2003's (FACTA), the Gramm-Leach-Bliley Act of 1999's (GLBA) Privacy Rule (GLBA Privacy Rule), the Bank Secrecy Act of 1970 (BSA), various anti-money laundering (AML) regulations, and the Children's Online Privacy Protection Act of 1998 (COPPA). In general, these U.S. federal laws and regulations strengthen the rights of individuals (particularly with respect to notice and disclosures of the fund's collection, use and disclosure of personal information) and mandate stricter controls over the processing of personal information by both the fund as a controller and the fund's vendors as processors of personal information.

In addition to this mosaic of privacy financial regulations, there is an intricate enforcement matrix for which federal agencies are responsible for each regulation. For example, GLBA is enforced by the FTC, the CFPB, the SEC, other federal regulatory authorities and state insurance regulators. The FTC has jurisdiction over any financial institution not regulated by other government agencies. The FCRA is enforced by the FTC and the CFPB. COPPA is enforced by the FTC.

In addition to these existing regulations, and as discussed in Part One of this series, in early 2022, the SEC proposed new rules that will increase the disclosure obligations related to cyber incidents that target U.S. registered investment advisors and funds. The SEC's proposed rules also expedite the notification periods to report to the SEC. Although the final form of the proposed rules is not finalized, it is highly likely that some increased cyber incident disclosure will apply before the end of 2023.

U.K.

In the U.K., disclosure requirements are created by the existing Principles of Business published by the U.K.'s Financial Conduct Authority (FCA). Under Principle 11, authorized firms (which include English registered funds and regulated English investment advisers as well as any regulated portfolio companies, as the payment provider business in our hypothetical would be if it operated in England) are required to deal with the FCA in an open and cooperative way and to disclose to the FCA anything relating to the firm of which the FCA would reasonably expect notice.

The FCA's Supervision Manual, especially at SUP 15.3, makes clear that a firm must immediately report all matters having a serious regulatory impact, which includes "*any matter which could affect the firm's ability to continue to provide adequate services to its customers and which could result in serious detriment to a customer of the firm.*" In practice, a regulated firm must report all material operational incidents to the FCA. A cyber incident may meet this threshold if it is an incident that results in a significant loss of data or in the unavailability or control of the firm's IT systems, affects a large number of customers or results in unauthorized access to, or malicious software being present on, the firm's information systems.

A fund may need to make a disclosure even if it has not been attacked itself, but if the victim was one of its portfolio companies. This is because the FCA guidance on Principle 11 requires that the firm "*takes into account the activities of other members of its group*". When drafting a notification, the

fund should consider whether any other agencies are being notified (see below), what action has been or is to be taken, both immediately and in the future, to ensure that such an attack cannot occur again.

The enforcement powers of the FCA are very broad. While fines are the most common sanction (and are unlimited), the FCA may also vary or cancel a firm's regulatory authorization, impose public censure or administer private warnings.

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

Money Laundering Considerations

U.S.

In the U.S., financial institutions subject to anti-money laundering requirements under the Bank Secrecy Act must file a SAR with the Financial Crime Enforcement Network (FinCEN), an agency of the Treasury Department, to report the cyber-event and the payment of any ransom. It is important to note that while both the U.K. and U.K. anti-money laundering regimes use the term "SARs", they must not be considered synonymous. SAR filings in the U.S. are different from those in the U.K. under POCA. Under the U.S. Bank Secrecy Act, filing a SAR does not confer any protection from a future money laundering offense, but the failure to file one can be, by itself, a regulatory violation resulting in civil, and potentially, criminal liability. Due diligence and critical assessment of the payment are therefore of paramount importance.

U.K.

A business based in the U.K. must consider whether the payment of a ransom is captured by the U.K.'s Proceeds of Crime Act 2002 (POCA) which captures potential money laundering offences. In short, it is an offense to enter into an arrangement where the payee knows or suspects such payment will facilitate the use of criminal property by another person. There are associated offences relating to tipping off and failure to report. It may be possible to obtain consent for such payment from the U.K.'s Serious Organised Crime Agency (SOCA) but such consent is granted only on a case-by-case basis and would require a business subject to a ransomware attack to engage with SOCA as soon as possible and prior to any payment.

U.K. financial institutions and other regulated businesses (which can include an English fund adviser or manager, regulated portfolio companies, as well as certain responsible individuals) will be under a duty to report potential instances of money laundering or terrorist financing (suspicious activity reports, or SARs) to the U.K.'s National Crime Agency (NCA) where they know, suspect or have reasonable grounds to know or suspect another person is engaged in such activity. Making a SAR can allow a firm and related individuals a defense to a substantive money laundering offence, if the NCA expressly gives consent to make the payment in question or by the effluxion of a specified time pe-

riod with no response from the NCA. The NCA can prove very responsive to concerns raised, especially in the context of cyber ransom demands.

Breach Notification Laws

U.S.

In the U.S., data protection notification laws are governed by a patchwork of state and federal laws. Despite proposed legislation (*e.g.*, American Data Privacy and Protection Act), there is currently no comprehensive federal law regulating privacy and the collection, use, processing, disclosure, and security of personal information. All 50 states, the District of Columbia, Guam, Puerto Rico and the Virgin Islands require businesses to notify individuals of security breaches of information involving personally identifiable information. Generally, U.S. data protection and breach notification laws consider personal information to include name combined with Social Security number, driver's license or state ID and account numbers.

In addition to the breach notification laws, a few states, including California, Colorado, Virginia, Utah and Connecticut, have comprehensive privacy laws, which may impose additional obligations when a fund experiences a ransomware attack**.** For example, the California Consumer Privacy Act (CCPA), provides for enhanced privacy protections for California residents, a private right of action for data breaches and statutory civil penalties up to $2,500 for each violation or $7,500 for repeated intentional violations after due notice and a 30-day cure period.

U.S. data protection or breach notification laws are typically triggered by "computer-security incidents". Each state and federal regulator defines such incidents, but most definitions include a common principle that it is an occurrence that results in harm to the confidentiality, integrity, or the availability of an information system or the information that the system processes, stores, or transmits. Although every ransomware attack needs to be analyzed based on the facts, circumstances and potential compromises to the fund's information system and personal information, most successful ransomware attacks will meet the definition of computer-security incident.

U.K.

In the U.K., if "personal data" (meaning data relating to natural persons from which they could be identified) has been accessed, exfiltrated or rendered unavailable, these are potential triggers for notifications to the Information Commissioner's Office (ICO) under U.K. GDPR (the U.K.'s implementation of the EU's General Data Protection Regulation 2016/679). If the ransomware incident meets the applicable threshold for notification, then the ICO may need notified to be notified "without undue delay" (and where feasible within 72 hours of the business becoming aware of relevant notifiable personal data breach).

Any entity that holds personal data will also be required to take appropriate technical and organizational measures to keep personal information secure and to restore information in the event of an

information security incident. Assuming that the payments provider company holds personal data, it must report any breach likely to result in a risk to individuals' rights and freedoms to the ICO within 72 hours, and if the risk to rights is a high one, also to the individuals involved. When determining its response, and setting any penalties for any data protection failings (which can be up to GBP 17.5 million or 4 percent of annual global turnover), the ICO will consider actions taken to mitigate the risk of harm to individuals involved in a data breach. Failure to report can attract its own penalty of GBP 8.7 million or up to 2 percent of global turnover.

Portfolio companies may be subject to additional or separate sectoral regulatory and notification regimes with respect to ransomware and cybersecurity incidents.

As a payment services provider, the portfolio company here will have some sector specific obligations – for example if it processes card payments it must comply with the industry standards set out in Payment Card Industry Data Security Standards in terms of notifying banks and credit card companies of fraud risks. Other industry sectors that may have additional compliance and notification requirements, include telecoms and digital service providers, essential services (which include energy, transport and health), suppliers to the government or defense sector and manufacturers, suppliers, and distributors of pharmaceutical or medical devices. Funds with investments in such sectors must therefore consider the full range of obligations on their investee companies.

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

Stakeholder Relationships

Finally, a fund or company has to consider its wider relationships, with investors, lenders, customers, suppliers and employees. There may be contractual requirements to notify counterparties of data breaches and cyber-attacks in addition to the contractual limitations on payments mentioned above.

In any event, as matter of reputation management, voluntary notification of the issue and remediation steps taken may help prevent further fraud, mitigate or contain losses, demonstrate good corporate citizenship and good faith to stakeholders, as well as being expected by regulators.

From the perspective of the sponsor, disclosures may be required in subsequent PPMs and marketing for any further fund raisings.

See "Defending Against the Rising Threat of Ransomware in the Wake of WannaCry" (May 31, 2017).

Consequences of a Ransomware Incident

A ransomware incident at the fund or its portfolio companies, whether malicious in nature or through inadvertent transmittal or other loss of data, can potentially jeopardize the fund's employees' or clients' or counterparties' sensitive, confidential, proprietary and other information processed and stored in, and transmitted through, the fund's computer systems and networks or those

of the fund's third-party service providers, or otherwise cause interruptions or malfunctions in the fund's, the fund's clients or third parties' operations.

A ransomware incident could result in material financial losses, increased costs, disruption of the fund's business, and liability to clients, and reputational damage. If the fund fails to comply with relevant data protection and breach notification laws and regulations or fails to provide the appropriate regulatory or other notifications of breach in a timely matter, state, federal and international regulators may open investigations and levy material monetary penalties and fines.

The fund and its portfolio companies may also face follow-on claims from customers, suppliers and partners. In addition to the immediate costs of investigating and resolving the cyber-attack, fines and other sanctions as well as claims for compensation can amount to very significant sums, even before factoring in reputational damage. Another consideration to note, under the U.K. GDPR, funds that exercise "decisive influence" with respect to the data protection compliance of their portfolio companies could be directly subject to regulatory fines under the U.K. GDPR. This is independent of liability of the infringing portfolio company.

Separate from regulatory enforcement, funds and their portfolio companies may be subject to private litigation arising from ransomware incidents, including investors, customers, suppliers and other partners.

While the U.K. government declined to introduce a class action regime for data protection, following a consultation in early 2021, the position as to whether class action-type claims may be commenced under the U.K. GDPR and the U.K. 2018 Data Protection Act remains unsettled. In the U.S., as night follows day, consumer class action lawsuits are filed within hours of many significant data breach.

Preventing the Next Breach

Following such a significant systems breach, the fund and all its investee companies should also review and update their cybersecurity risk assessments, incident response plans and systems in line with the latest guidance, policy frameworks and expectations on operational resilience, cybersecurity and data protection from applicable regulators (in the U.K., the FCA and ICO will be key, and in the U.S., the proposed SEC rules), as well as current industry best practice. They may also wish to work with advisers to understand how they came to be a victim of ransomware, and to ensure that they have understood the cyber security implications and taken steps to protect themselves from similar incidents. Such actions could provide a mitigating factor in the eyes of regulators such as the U.K.'s ICO in any future incidents.

As ever, though, the best form of defense is to ensure strong systems and controls, as well as constant vigilance to avoid becoming a target and victim in the first place. Policies must be living documents, subject to regular updates and review, with third party led resilience testing as well as practice at incident response. Cybersecurity risks and preparation should be a matter for proactive

board oversight (including any sponsor-appointed directors) who must have the relevant skills and training.

See "Ransomware Lessons From the Trenches of the MedStar Attack" (Jul. 11, 2018).

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.