King & Spalding
Client Alert

Cyberattack and Ransomware Attack Force Majeure Considerations

MAY 20, 2021

For more information, contact:

Elizabeth Silbert
+1 404 572 3570
esilbert@kslaw.com

Phyllis Sumner
+1 404 572 4799
psumner@kslaw.com

Elizabeth Adler
+1 404 572 3555
eadler@kslaw.com

Tim Lee
+1 404 572 3577
tlee@kslaw.com

Charlie Spalding
+1 404 572 4666
cspalding@kslaw.com

King & Spalding

Atlanta
1180 Peachtree Street, NE
Suite 1600
Atlanta, GA 30309-3521
Tel: +1 404 572 4600

As criminal cyberattacks and ransomware attacks on critical infrastructure increase, companies may experience significant business disruptions. Ransomware and cyberattacks may prevent companies from fulfilling contractual requirements for the supply of product. Such attacks may also force companies to make difficult decisions regarding how to allocate a limited supply of product when replenishment is uncertain. In these circumstances, companies should consider: (1) whether a ransomware or cyberattack constitutes a "*force majeure*" under their contractual provisions; (2) whether any other doctrines may excuse performance; and (3) how they might allocate their limited supply of product to customers.

Question 1: Does a cyberattack or ransomware attack constitute *force majeure*?

Companies seeking to invoke *force majeure* must demonstrate that the ransomware attack or cyberattack at issue is within the scope of the *force majeure* provision. The specific language of a *force majeure* provision is the most important consideration when evaluating whether a particular event excuses performance. *See generally Kel Kim Corp. v. Cent. Mkts., Inc.*, 519 N.E.2d 295, 296 (N.Y. 1987) ("Ordinarily, only if the *force majeure* clause specifically includes the event that actually prevents a party's performance will that party be excused."); *Kyocera Corp. v. Hemlock Semiconductor, LLC*, 886 N.W.2d 445, 446 (Mich. Ct. App. 2015) (explaining that general rules of contract interpretation apply to *force majeure* clauses).

Some provisions may specifically reference cyberattack, terrorism, sabotage, or third-party criminal conduct as a *force majeure* event. *See, e.g.*, *Rochester Gas & Elec. Corp. v. Delta Star, Inc.*, No. 06–CV–6155–CJS–MWP, 2009 WL 368508, at *2 (W.D.N.Y. Feb. 13, 2009) (*force majeure* clause expressly included "sabotage, terrorism, [and] vandalism"). When a *force majeure* provision enumerates particular categories of events, the specific nature of the attack, including the identity and motives of the perpetrators, may be relevant to determine whether the attack

qualifies. Other *force majeure* provisions might be phrased broadly to include any event beyond the contracting party's "reasonable control." When a contracting party relies on a "reasonable control" provision, whether the party took reasonable efforts to prevent the attack may be a relevant factual inquiry.

Few courts have addressed whether a ransomware attack or cyberattack constitutes a *force majeure* event. Some courts have indicated—although not conclusively—that such an event would likely qualify as a *force majeure* event. *See, e.g., Princeton Cmty. Hosp. Ass'n, Inc. v. Nuance Commc'ns, Inc.*, No. 1:19-00265, 2020 WL 1698363, at *5 (S.D.W.Va. Apr. 7, 2020) (assuming but not deciding that Russian-launched malware attack was an act of terrorism, act of war, or a governmental act or order for purposes of *force majeure* clause); *Heritage Valley Health Sys., Inc. v. Nuance Commc'ns, Inc.*, 479 F. Supp. 3d 175, 184 n.4 (W.D. Pa. 2020) (stating in dicta that "a cyber-attack launched by the Russian government which affected many other companies and organizations worldwide – was arguably beyond [Defendant's] reasonable control"). A court's analysis, however, will depend primarily on the language of the relevant *force majeure* provision, rather than general authority characterizing cyberattacks as *force majeure* events.

Question 2: What other doctrines might excuse non-performance?

Companies should also consider the impact of the doctrines of impossibility or frustration of purpose after a ransomware attack or a cyberattack. The specific features of these doctrines vary by state. But generally speaking, excuse under such doctrines requires that an unforeseeable event make a party's performance impracticable or impossible, by no fault of that party. *See generally* Restatement (2d) Contracts § 261 (discussing impracticability); *id*. § 265 (discussing frustration of purpose). A company whose business is interrupted as a result of a ransomware or cyberattack may seek to excuse performance under these or other common-law doctrines.

Question 3: How should companies allocate limited supply?

Finally, companies should consider how to approach downstream obligations when faced with insufficient supply. First, companies should consider whether their *force majeure* clause specifies how to allocate performance in such a circumstance. *See, e.g.*, *PT Kaltim Prima Coal v. AES Barbers Point, Inc.*, 180 F. Supp. 2d 475, 480 (S.D.N.Y. 2001) (contract expressly required allocation of coal supplies on a pro rata basis with contracted customers in event of *force majeure*). In the absence of a clear obligation to allocate supply in a particular way, companies should be aware that their allocations may create conflicts with customers seeking to maximize their shares of the limited supply available. For example, if a company fully performs for some downstream customers but not others and seeks to excuse its non-performance based on *force majeure*, dissatisfied customers may claim that the company's failure to provide them with at least partial performance was the result not of a *force majeure* event, but of the company's decision to allocate available limited supply in a particular way. *See* Williston on Contracts § 77:99 ("Where a promise becomes impossible but only in part, a promisor is not excused from performing the balance of the agreement that can still be accomplished despite this partial commercial frustration."). Thus, *force majeure* may not excuse complete non-performance if a company could have partially performed but instead chose to allocate performance elsewhere.

ABOUT KING & SPALDING

Celebrating more than 130 years of service, King & Spalding is an international law firm that represents a broad array of clients, including half of the Fortune Global 100, with 1,200 lawyers in 22 offices in the United States, Europe, the Middle East and Asia. The firm has handled matters in over 160 countries on six continents and is consistently recognized for the results it obtains, uncompromising commitment to quality, and dedication to understanding the business and culture of its clients.

ABU DHABI	CHARLOTTE	FRANKFURT	LOS ANGELES	PARIS	SINGAPORE
ATLANTA	CHICAGO	GENEVA	MOSCOW	RIYADH	TOKYO
AUSTIN	DENVER	HOUSTON	NEW YORK	SAN FRANCISCO	WASHINGTON, D.C.
BRUSSELS	DUBAI	LONDON	NORTHERN VIRGINIA	SILICON VALLEY	