KING | FISHER
LAW FIRM

COVID-19 Special Newsletter

¤ April 24, 2020 ¤

The COVID-19 (or novel coronavirus) pandemic is upon us. It goes without saying that these are strange and unusual times – for nations, businesses, attorneys and contract professionals, and everyone else. In particular, for attorneys and contract professionals, the pandemic will stretch how we draft, negotiate, implement, and manage technology and other commercial agreements. In this newsletter, we identify several potential considerations and impacts of the COVID-19 crisis on technology and other commercial transactions. These items and this discussion are by no means exhaustive, but we nonetheless hope you find it helpful.

* * * * * * * *

Software License Terms. Countless businesses across the U.S. have voluntarily or by legal mandate begun requiring their employees to work from home. Often over-shadowed by the cyber security risks related to working from home (see below) are the software license terms that apply to or prohibit use of business-licensed software by employees at home. Depending on the scope of the uses licensed – enterprise, per-seat, concurrent-use, *etc.* – your employees' use of company-licensed software at home may be problematic.

Be sure to carefully review your company's software licenses (and other technology licenses) in order to identify and assess these risks. Many software licensors have terms and conditions that speak specifically to (or against) "home use," including, as a *very* short list of examples, Autodesk, Future Corporation Software, JNBridge, Sophos, and WebWorks.

Similarly, be sure that your contracts with cyber security vendors for endpoint protection reach any new devices that your employees may be using to work from home.

Force Majeure. It is likely that you or the parties with which you contract have raised the possibility that COVID-19 is or has caused a force majeure event excusing performance under the contract. Many of our clients have begun assessing their contracts to identify and evaluate one or more parties' rights in this regard.

If your contractual performance is at risk, consider investigating whether relying on force majeure may provide help. Generally speaking, force majeure is a state law issue and is strictly a matter of contract law and interpretation (that is, not common law). Thus, the precise language of your particular force majeure provision, as well as the governing law, are critical. If the clause lists particular events of force majeure, it is important to note whether it references only acts of God or acts beyond the reasonable control of the parties, or whether it specifically lists occurrences such as pandemics, epidemics, diseases, quarantines, labor shortages, government actions, or laws or orders. As you review the language, be sure to keep an eye out for catch-all language, the effect of which may be limited by foreseeability, and to the rule of *ejusdem generis* regarding the interpretation of clauses listing a string of items. Also pay close attention to any notice or similar requirements in the force majeure clause. TEC Olmos v. ConocoPhillips, 555 S.W.3d 176 (Tex. App. 2018) is a very informative case on force majeure under Texas law.

For transactions in goods in Texas, you may also be able to rely on Tex. Bus. & Com. § 2.615, which regards excuse by failure of presupposed conditions. Parties contemplating force majeure often simultaneously consider the applicability of

the legal concepts of frustration, impossibility, and impracticability.

Contract Renegotiation. Even if COVID-19 is not a force majeure event impacting your non-performance under a particular contract, the current pandemic may nonetheless be affecting your ability – or desire – to perform. The cost pressures currently facing nearly all businesses are palpable. In addition, whether or not directly affecting performance-based terms in your agreements, the effects of the pandemic may also impact contract terms regarding business continuity and disaster recovery, warranties of compliance with and performance under other agreements, the meaning of "commercially reasonable efforts," the definition of "business days," and severability and "blue pencil" language. Consider how you fare under the contract, as a whole.

Whether to reduce your costs and fees over the short or medium term or to extend the time needed for performance – or even to secure greater benefits or additional products, technology, or services – consider whether the current environment is an appropriate time to seek to renegotiate key or otherwise impacted contracts. In some cases, for example, it can work to both contracting parties' advantage to reduce annual costs and fees, while extending the duration of the contract.

You would not be the first company to try to renegotiate contract terms. UAW recently has, and Wells Fargo did last year for other reasons.

Cyber Security. With so many employees now working from home, along with the expected migration of businesses from local to cloud-based environments due to corporate budgetary constraints, cyber security risks to employer operations and data have significantly increased during the COVID-19 pandemic. For IT departments, there are numerous sources of available guidance – from the complex (e.g., NIST), to the middle-of-the-road (e.g., Sentinel One), to the simple (e.g., FTC). The FBI has even issued Zoom-specific guidance.

For in-house attorneys and contract professionals, look at other avenues to mitigate or address heightened cyber security risks –

- Review your company's cyber security and other insurance policies to see how they address the increased risk profile. Although it is possible that your insurers will not embrace renegotiating deficient policies in the present environment (unless you're renewing your coverage), the review may help you identify gaps in need of prompt solutions – whether the solutions are operational or involve other paths or resources.
- Review your contracts with data security and other technology vendors and providers to identify cyber security-related reports and information that are due your company. Especially where permitted or required by your contracts, you may be able to identify and avoid the impacts of impending cyber security exposures by requesting copies of required (or even available) SOC reports, other third-party audit reports, and certificates of insurance.
- Develop, conduct, or provide internal business counsel as to the value of enhanced employee training on cyber security matters, in particular including phishing, unsolicited commercial emails (including those offering updated information about COVID-19), business email compromise, shadow IT, and adhering to company IT policies.

Should you have any questions as to any of these items, please don't hesitate to reach out to us.