masuda funai

News & Types: Client Advisories

Three Critical Issues in the Area of Commercial Litigation and Dispute Management

3/30/2022

Practices: Litigation

DEFENDING BREACH OF CONTRACT CLAIMS ARISING FROM SUPPLY CHAIN DISRUPTIONS:
Significant disruptions in supply chains increased for many industries in 2021 and there is no indication that these disruptions will be decreasing anytime soon. This means American manufacturers and distributors are facing increased pressure from customers to deliver product within promised deadlines. Many companies were initially reluctant to file lawsuits in the early phases of the COVID-19 pandemic to enforce contract terms and most U.S. courts reduced or suspended altogether regular court functions in 2020 and the early portion of 2021.

With the COVID-19 pandemic entering its third year, businesses have lost patience with the shortages that have crippled them for two years and the threats of litigation and the filing of commercial litigation has seen an uptick in the past several months. Many companies are no longer willing to “wait their turn” for goods and services that were promised to be delivered months or even over a year ago.

Companies should now be prepared to face claims from their customers for missed delivery deadlines and for product shortages. Defending such claims requires companies to review their important business relationships – even long-standing ones – and revise contracts when possible to avoid promising too much. Most importantly, if customers begin making threats of filing lawsuits or arbitration claims, consult with your business attorney as soon as possible to see if effective defenses can be developed and asserted **before** a lawsuit is filed. Timing is everything in business and in litigation.

Make sure you discuss the pre-litigation steps you intend to take with your experienced litigation counsel.

DEFENDING CLAIMS RESULTING FROM CYBER ATTACKS ON YOUR COMPUTER FILES AND SYSTEMS:
There has also been a significant rise in the number of hacking and phishing schemes perpetrated against non-public companies and businesses in the U.S. The range and depth of these schemes varies, but even a simple phishing scheme – if successful – can result in claims by your customers and suppliers for breach of contract or violation of state privacy laws. One of the most common phishing schemes begins with an e-mailed request by a long-time supplier to change how its invoices are paid. Of course, the source of the request is not the actual supplier, but somebody who has cleverly made their phishing e-mail look authentic. It’s so easy for a

busy company to inadvertently fall victim to this scheme, and if successful, the phisher keeps issuing fake invoices from different suppliers until the ruse is discovered. There are dozens of variations on this scheme – most require no actual hacking of the company's files – just a fake e-mail address and maybe a phone call.

A more sophisticated cyber-attack – usually initiated far from the reach of U.S. police – does require the hacking of the company's computer systems and files. This can often be accomplished faster than you might expect; the hacker only has to find access through a single vulnerable point in order to take control of the company's systems and confidential files, including financial data and customer information. Hackers then lock you out of your systems and threaten the public release of your highly confidential information if a ransom is not paid. Managing cyber-crime incidents – while they are ongoing – and then promptly addressing claims that may result from the possible release of personal information, or for the expenses and damages that customers and suppliers may incur as a result of the incident, is critical to a company's reputation and, in some instances, even its survival.

Make sure your company is prepared to defend both cyber-attacks and the claims that quickly follow.

LITIGATION DIRECTED AT ENFORCING AND DEFENDING EMPLOYEE NON-COMPETE AND NON-SOLICITATION AGREEMENTS:

A very tight job market means that companies will continue to lose valuable employees to competitors. Such departures also put critical customer and supplier relationships at risk, as well as create the potential for the disclosure of confidential information. Companies have traditionally sought to protect the "poaching" of their employees through employee "Non-competition, Non-solicitation and Confidentiality Agreements." Lawsuits to enforce such agreements are on the rise in the U.S. but the states don't have a uniform approach to the enforcement of such contracts after an employee departs. And perhaps because of the pandemic, some courts are looking less favorably on the enforcement of such contracts. A host of factors will impact whether a court will enforce your former employee's promise to not join a competitor and to not solicit the customers he called on for you. The time for assessing these factors is before the employee departs. An annual review of your employee "non-compete/non-solicitation" agreements and the company's practices with respect to protecting customer relationships and confidential information is absolutely necessary in 2022, especially since some states are implementing restrictive new legislation and penalizing companies for non-compliance. Such a review and potential changes to company practices and employee contracts should be conducted with the help and advice of your attorneys to ensure a court will recognize and enforce employee commitments.

Please reach out to your Masuda Funai relationship attorney or one of the attorneys in the Firm's Litigation Department for more information on any of these topics or litigation issues.