

Managing Contract Liability in Ransomware Disruptions: A Case Study in the Logistics Sector

May 16, 2024

By Mark G. Wenda, IV



Recent litigation in the State of Washington highlights the need to address the evolving landscape of cyber liability and ransomware attacks. The lawsuit filed by POC USA, LLC ("POC") against Expeditors International of Washington, Inc. ("Expeditors") stems from a failure to fulfill third-party logistics services during a ransomware attack. The rising prevalence of ransomware is a concern that all businesses should address in their agreements. Because this litigation pertains directly to shipping fulfillment centers, we want to address how industry stakeholders can proactively address these cyber liability and ransomware issues in their service agreements.

For context, POC manufactures and distributes protective gear for gravity sports such as skiing and mountain biking. Expeditors, on the other hand, is a third-party logistics ("3PL") provider. Expeditors contracted with POC and agreed to handle POC's shipping and distribution of protective gear.

Expeditors suffered a ransomware attack that disrupted their ability to provide 3PL services for 90 days. Consequently, POC filed suit seeking the recovery of damages stemming from lost revenue resulting from the ransomware attack. POC's complaint includes a claim for:

1. Breach of Contract
2. Breach of Implied Covenant of Good Faith and Fair Dealing
3. Washington Consumer Protection Act Violations
4. Unjust Enrichment
5. Negligence and Gross Negligence

In response, Expeditors filed a motion to dismiss, seeking a court order dismissing POC's claims.

On April 11, 2024, the court issued an opinion and order, dismissing the claims of negligence, gross negligence, and bailment. However, POC's claims for breach of contract, breach of implied covenant of good faith and fair dealing, unjust enrichment, and Washington Consumer Protection Act violations were not dismissed remain subject to litigation.

This pending litigation highlights the need to analyze and update commercial agreements to address current events that may cause service disruptions, such as ransomware. Failing to properly address these disruptions in your commercial agreements could leave your organization vulnerable to significant and unexpected claims.

In today's business environment, it is essential for almost every company to proactively review and update their agreements to

address cyber liability and ransomware concerns effectively. The only exception would be a business run entirely on offline systems, a rarity today. Below are some of the relevant clauses to examine:

Limitation of Liability:

While many agreements limit liability to only the consideration paid under the agreement, the exact text of that clause matters. The language of that limitation of liability clause may not limit certain claims asserted for loss of services stemming from a ransomware attack. Based on the business operations, it may be prudent to ensure that your distribution services agreement does not limit liability solely to damages stemming from property damage (thereby allowing unlimited liability for claims other than property damage). At a minimum, the language should be updated to expressly limit liability for damages resulting from a loss of services due to uncontrollable events. This issue should also be addressed in your force majeure clause, as discussed in the following paragraph. By addressing this in the force majeure clause, cyber-attack liability can be effectively limited. This approach is preferred because, as illustrated in the case of *POC v. Expeditors*, where the amount paid under the agreement in prior years was \$2.5-3 million, each company should endeavor to avoid any damages stemming from the malicious acts of a third party.

Force Majeure:

The force majeure clause is another critical clause that must be updated to address these issues. Relying on a contract's limitation or disclaimer of liability clause is insufficient. The force majeure clause should expressly identify a force majeure event to include a loss of access or inability to perform services due to cyber-attacks, ransomware attacks, or other malicious third-party attacks on your cyber infrastructure, including hardware, on-premises, and cloud-based systems of any kind.

Warranties and Representations:

One of the factual averments set forth in the *POC vs. Expeditors* litigation focused on Expeditors' representation that it used "up-to-date tools" that enabled Expeditors to move cargo "securely." Arguably, Expeditors' reference to "security" may mean *physical* security. Still, the lack of clarity opened Expeditors up to litigation based on this representation, including *cyber* security. A better approach to representations regarding cyber security should include a "commercially reasonable" qualifier. Companies should also audit their marketing material to ensure no marketing copy is overcommitting your organization to provide best-in-class cyber security, especially when that is not the case.

Catch-All Disclaimers:

Additional language expressly disclaiming the ability to perform services in the event of a cyber-security or ransomware attack is a widely accepted and prudent way to avoid claims from your customers. These clauses may be heavily negotiated but should be a baseline starting point for every 3PL service provider, providing a sense of industry-standard security.

Cyber Insurance:

Cyber liability insurance is another consideration to examine outside of the contract terms. Many service agreements now require that all parties maintain a cyber liability insurance policy; however, these policies are becoming increasingly expensive. The cost of insurance premiums also depends on the security measures your business puts in place, so engaging a cyber security professional is also a prudent method to mitigate cyber liability exposure and reduce insurance premiums.

The above list is not exhaustive, and every organization will have scenarios that require bespoke contract language to address (and mitigate) potential customer claims. Engaging competent legal counsel capable of crafting the appropriate language within your agreements is crucial to ensuring comprehensive protection.