Wolters Kluwer

Conflict in Ukraine: Confronting contract risks and obligations

SPECIAL REPORT | The Ukraine Crisis

The Russian invasion of Ukraine has been a sudden, and dramatic, disruption for companies doing business with companies or persons in Eastern Europe, especially for those doing business in Ukraine or Russia. In addition, the voluntary withdrawal of many companies from those markets has contributed to the disruption, so that it is now virtually impossible to continue business in those countries. The legal and financial consequences of this disruption are serious. Many companies, especially smaller companies, are in unfortunate positions. There are, however, legal and insurance options that may mitigate or minimize these consequences.

FORCE MAJEURE

When business relationships are made, they rely on assumptions as to what is likely or probable to happen in the future. These assumptions are often not made an explicit part of an agreement but underlie everything. When events upend those assumptions, it may be impossible for the relationship to continue as planned. That type of event is a *force majeure*, or superior force. A *force majeure* is an event outside the control of a party to the contract. Common examples of *forces majeures* include natural disasters, pandemics, or war.

The question of *force majeure* as an impediment to the performance of an agreement has taken on a new currency recently, first due to the COVID-19 pandemic, and more recently with regard to Russia's invasion of Ukraine and the sanctions that have been imposed in response to that invasion. A number of American companies have contracts with vendors in Eastern Europe, including Russia and Ukraine. If these vendors are unable to continue to work in support of their contracts with American companies, what will happen?

Many contracts contain *force majeure* clauses that set out what happens in the event of an occurrence making performance of a contract impossible. These clauses may, however, define the term *force majeure* in a way that excludes war or economic sanctions in response to war. For example, a common definition is that *force majeure* is limited to "acts of God." An act of God is understood to mean an event not caused or controlled by humans. War would not be included in the limitations of this definition.

Other *force majeure* clauses include governmental action, including "acts of a civil or military authority." This definition would obviously include acts of war. Some clauses have a catch-all definition that would include "any cause outside the control of a party hereto." It is likely that such a clause would be held to include an act of war.

If there is no such clause, a party seeking to excuse their inability to perform could rely on the doctrine of impossibility of performance. Proving impossibility may be difficult. Impossibility will excuse non-performance only if performance is objectively impossible; that is, performance of the contract by anyone is impossible. If there is any alternate means for a contract to be performed, impossibility will not excuse performance.

FRUSTRATION OF PURPOSE

A doctrine related to impossibility is the doctrine of frustration of purpose. Frustration of purpose will excuse performance when a party's principal purpose in making a contract is frustrated without that party's fault, by the occurrence of an event, the non-occurrence of which was a basic assumption on which the contract was made.

Most agreements are made with at least the tacit assumption that war will not break out, and that economic sanctions will not be imposed. The disruptions of war and of sanctions imposed in response will certainly frustrate the purpose of a contract. Frustration may provide an excuse for non-performance that the doctrine of impossibility would not.

RISK ALLOCATION

Most commercial agreements contain some type of risk allocation provision. Indemnity clauses, limitations of liability,

and liquidated damages are all examples of contractual risk allocation provisions.

Risk allocation is typically negotiated and built into a contract. It may be done through a risk allocation clause or clauses, or the allocation of risk may be determined by law. In some instances, such as contracts for the sale of goods, risk allocation is often determined by terms of art used in the contract. In other instances, the allocation of risk will be determined by the law relating to the performance or non-performance of the contract. The legal consequences of a breach of contract may be thought of as risk allocation that has been determined without the input of the parties.

SUPPLY CHAIN DISRUPTIONS

Supply chain disruptions provide a good example of the type of outside causes that can make it difficult for a business to function. An inability to obtain necessary supplies or materials is an event outside the control of a party that was assumed would not happen. This could lead to a claim of frustration of purpose.

The risk of supply chain disruption is something that could be allocated at the time a contract is negotiated. Parties could, for example, agree to forfeit all or part of any advance payments made in the event outside events interfere with the supply chain. Of course, for such a clause to be included in a contract, the parties would have to anticipate the possibility of it happening.

BUSINESS INTERRUPTION AND CYBER INSURANCE

Business interruption insurance – also referred to as business income insurance – aims to protect companies against losses incurred when certain perils temporarily force them to shut down. As a general rule, business interruption policies cover continuing operating costs and protect against income loss. Policies will pay for lost profits, mortgage, rent, or lease payments, employee salaries, loan payments, and taxes during the time a business is unable to operate.

To be covered, the business's losses must be caused by direct physical damage to its property. In addition, the cause of such damage must fall within the covered dangers such as fire, or weather conditions.

Such insurance can be obtained on its own, or as an add-on to a commercial property insurance policy. Small and medium-sized businesses may have a business owner's policy – a specific form of bundled insurance coverage – that includes business interruption insurance.

Some other underlying causes, such as earthquakes and floods, will usually only be covered if a business's commercial property insurance specifically covers them.

Cyber insurance is a relatively new form of insurance. Because it is new, it is difficult to say what a "typical" policy will cover. Depending on the policy, coverage may be provided for cyber extortion ("ransomware"), or business interruptions linked specifically to cyber incidents such as a network attack that interferes with a company's ability to operate. Other areas of coverage include the loss or corruption of data or even the broader consequences of cyber incidents, such as the public relations crises they may trigger, or the need to notify affected customers. Policies that cover risks unless they are explicitly excluded are also available.

Business interruption and cyber insurance are generally available as part of product packages or as a stand-alone product. Specialized policies tailored to the needs of one policy holder, may also be available.

WAR RISK INSURANCE

Business interruption and cyber insurance typically exclude losses caused by acts of war. War risk insurance is insurance that is limited to providing coverage for losses caused by war, insurrection, or terrorism. War risk insurance is, however, generally limited to transportation industries, such as shipping companies or airlines.

TACKLING RISK

The potential implications for businesses are equally dizzying. A company may be using a vendor located in Ukraine or in Russia, rely on supplies that need to be transported to or from these countries, or may own property there. Or it may simply have spoken out against the invasion, and may be wondering whether this will draw the ire of hackers.

Indeed, the current crisis may trigger risks for businesses that are as diverse as the specific insurance policies they may be holding. Ultimately, concrete advice will need to be based on special attention to a client's individual circumstances.

Still, some steps are sensible regardless of the specific business realities or insurance policy details. Proactively reviewing your insurance policies and their exclusions, and seeing whether you can re-negotiate coverage or need to obtain expanded coverage is vital. Take a closer, and perhaps newly clear-eyed, look at your supply chain and its inherent risks. If you don't

have back-up suppliers and vendors, identify candidates now – and nurture your relationship with them. It's also a good time to scrutinize your business continuity plan, making sure it addresses supply chain disruptions and cyberattacks.

If you are anticipating interruptions, think both about how you will address the problem and about how and when you will communicate about it – internally, externally, and with specific clients. A professional assessment of your cyber security weaknesses may also be in order. At minimum, inform yourself about the – sometimes surprisingly basic – steps that can bolster protection. If you have cyber insurance, and actually suffer an attack, report it to your insurance broker immediately. ■