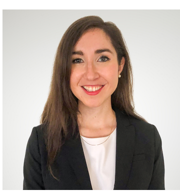
Snell & Wilmer
Committed to being your perfect fit.®

Brett W. Johnson
602.382.6312
bwjohnson@swlaw.com



Mary Colleen Fowler
602.382.6889
mfowler@swlaw.com

Snell & Wilmer
Past Issues

February 28, 2022

The Russia-Ukraine Conflict: Updated Sanctions, SWIFT Action, and Impact on Global Trade

By Brett W. Johnson and Mary Colleen Fowler

The international community continues to heighten the compliance burden for companies with business ties to Ukraine and Russia following a new round of sanctions. On February 26, 2022, the United States, along with several other countries, announced it would cut off certain Russian banks from the Society of the Worldwide Interbank Financial Telecommunication ("SWIFT") system. In addition, multiple countries that usually remain neutral, such as Switzerland, have joined in issuing sanctions against Russia. Although there may be some delay in the sanctions implementation, companies should consider continuing to take efforts to mitigate risk associated with existing and likely future sanctions against the Russian economy.

SWIFT is the primary means of a fast and secure messaging system that allows banks to issue and confirm cross-border payments for over 200 countries. The European Union and United States, among others, are working to finalize which banks will be impacted by the SWIFT sanctions. By sanctioning the selected Russian banks from SWIFT, the Russia Federation will be limited in its ability to liquidate assets held abroad and limit its ability to send and obtain money. The sanctions seek to cut off Russia's external sources of foreign funds and inhibit its ability to continue its war across Ukraine.

In light of the ever-increasing sanctions—the freezing of Russian assets, placing new limits on state-owned energy, logistics, and limiting shipping firms' ability to raise money, and instituting a blockade against technology limiting Russia's military and industrial capacity—companies should keep a close eye on the evolving Russian-Ukraine situation. Likely already familiar with sanctions issued in 2014 due to the Russian invasion of Crimea, companies should be mindful that the ramp-up of financial pressures in reaction to Russia's aggression may impact their business operations at several levels.

U.S. companies will likely face substantial exposure throughout their supply chains. To help mitigate this impact, companies should consider evaluating their force majeure provisions in contracts that may be impacted by the Russia-Ukraine conflict, and consider notifying customers and suppliers about potential disruptions. In many cases, the force majeure provisions have specific notification requirements which are at times overlooked. Companies will likely be in a better situation in future legal disputes with vendors and customers if they can point to compliance with contractual provisions, government guidance, and, most importantly, declarations and regulations.

Companies should also consider reviewing their policies and procedures—including those for increasing and updating screening entities and individuals against sanctions lists—to help ensure that contingency plans are in place. Even companies with developed response plans should consider reviewing their procedures to account for new sanctions and impacts on global trade (not just Europe). Specifically, consider ensuring that entities in the supply chain (including financiers and investors) are screened against the various denied parties' lists maintained by the United States, Canada and Europe. This includes transactions that have already been screened and are currently being performed, not just future business opportunities. This may be key to ensuring continuity of ongoing business operations.

Companies should also consider evaluating their export license requirements. The U.S. Department of Commerce's Bureau of Industry and Security ("BIS") created new license requirements for export control classification numbers ("ECCN") related to transactions with Russia. This will impact products exported, reexported or transferred to Russia. Companies should be aware that certain goods that previously authorized or otherwise dealt with innocuous products or services, may now be prohibited or require licenses under applicable export-import laws. As such, companies should consider taking this opportunity to confirm their products and services correct ECCN and that they are reported correctly on shipping documentation. Of note, depending on the origin of productions, multiple countries' export licenses may not be necessary. Companies that have been granted general licenses may have a short window to continue or wind down select transactions, but should expect these licenses to expire within the month. Ultimately, if they have not already, companies should build contingency plans for how to reorganize transactions involving Russia or Ukraine.

Additionally, the New York State Department of Financial Services ("DFS"), typically considered the gold standard for sanctions compliance enforcement, warns that companies could be at risk of Russian cyberattacks in attempts to evade the increasingly heightened sanctions. Notably, DFS highlights that cryptocurrency could allow designated banks and individuals to evade sanctions. It also recommends that companies with Russian or Ukrainian offices consider "segregating" those offices from their other global efforts as a security precaution. Thus, companies should keep abreast of changing sanctions and consider implementing appropriate internal controls, including risk assessments, testing against their risk profiles, and incorporating necessary training for those handling or accessing systems at risk to attack.

Companies must be mindful of the above risks, but also must consider the impacts of Russian law as they become compliant with newly issued sanctions. It is likely that Russian law will be implicated for breach of contracts, termination of Russian-based employees, or prohibition of repatriation of revenues and profits from branches or subsidiaries, among other things. Thus, just as companies ensure compliance with United States and EU laws, companies with operations in Russia must also evaluate risks associated with compliance there and address any conflicts and legal obligations.

The economic reaction to Russia's invasion of Ukraine indicates that compliance will be fully expected, and violations will not be taken lightly. Governments, including the U.S., have already indicated that a special task force will ensure implementation of the existing sanctions. Companies should expect more information about this task force in the coming days. The expected date for the additional regulator compliance is March 26, 2022. Companies should ensure their internal and external controls align with issued and future-issued sanctions.

As the rippling effects of these sanctions are yet to be fully felt due to the size and global impact of Russia's economy, Snell & Wilmer will continue to follow developments in the Russia-Ukraine conflict. Companies should consider reaching out to legal counsel to better understand the impact of the ever-changing economic sanctions, and the potential for additional sanctions, on their business opportunities and employee support.

Tweet!

Linked in

One Arizona Center | 400 East Van Buren Street | Suite 1900 | Phoenix, Arizona 85004