View on our website.

GIBSON DUNN

Mergers & Acquisitions and International Trade Update

October 16, 2024

Top International Trade Issues to Think About in M&A Deals

An overview of International Trade considerations that most frequently impact deal timing, valuation, and ability to operate after closing.

In today's global economy, geopolitical risks are on the rise and international trade controls are a tool of first resort deployed by the United States and other jurisdictions to achieve foreign policy and national security goals. International trade controls include financial and trade sanctions, export and import controls, national security reviews of foreign direct investment, and (anticipated) controls on outbound investment. These controls can have an impact on a target's valuation, ability to continue operating in the same manner or in the same jurisdictions as prior to an acquisition or affect deal timing and certainty. Liability for a target's past conduct can be imputed to the buyer in many circumstances, including for strict liability offenses.

In addition to potential civil and criminal liability, violations of international trade laws can result in other adverse consequences for buyers, including substantial reputational harm, costly government investigations or monitorships, or even halting the deal. Many acquisition targets—especially smaller, fast-growing targets—may lack adequate policies and procedures to mitigate the risk of violating applicable international trade laws. Therefore, it is critical to understand a target's risk profile, internal controls, and potential exposure to regulatory, commercial, and reputational risks during pre-acquisition due diligence.

1. Dealings with Sanctioned Parties and Sanctioned Jurisdictions

Whether a target is transacting business in violation of applicable U.S. sanctions is often a top concern for buyers and insurers alike. Unlike some other areas of the law, corporate formality in the structure of an acquisition will not always insulate a buyer from civil liability for past violations of the target. Rather, in enforcing U.S. sanctions, the Department of the Treasury's Office of Foreign Assets Control ("OFAC") is usually willing to "pierce the corporate veil." Nor will a buyer's lack of knowledge regarding the target's past sanctions violations necessarily shield it from liability. Even inadvertent violations of U.S. sanctions can result in substantial monetary penalties, at times in the tens of millions, and occasionally beyond. In April of this year, the statute of limitations for sanctions violations was expanded from 5 to 10 years.

Consequently, it is critical to focus on potential exposure to sanctioned persons or sanctioned jurisdictions during pre-acquisition due diligence. U.S. sanctions requirements can be understood to fall into two broad categories:

- Dealings with **sanctioned parties**: U.S. sanctions generally prohibit U.S.-linked business involving "blocked" persons or entities listed on OFAC's List of Specially Designated Nationals and Blocked Persons (the "SDN List"). Pursuant to OFAC's 50 Percent Rule, these broad prohibitions extend to entities owned 50% or more by blocked persons, whether directly or indirectly and whether by a single blocked person or in the aggregate.
- Dealings with **sanctioned jurisdictions**: U.S. sanctions generally prohibit U.S.-linked business involving "comprehensively-sanctioned" jurisdictions, which, as of this writing, include Cuba, Iran, Syria, North Korea, Crimea, and the so-called Luhansk People's Republic and Donetsk People's Republic regions of Ukraine.

In addition to direct prohibitions on U.S.-nexus dealings, U.S. persons are generally prohibited from "facilitating" foreign transactions that involve a sanctioned party or sanctioned jurisdiction. Consequently, it is essential to ensure that target companies with an international footprint have adequate policies and procedures in place to avoid and detect transactions that may be prohibited by applicable sanctions.

OFAC encourages companies to employ a "risk-based approach" in designing and deploying sanctions compliance programs (see OFAC's "Framework for Compliance Commitments"). Risk factors include a company's size and sophistication, products and services, customers and counterparties, and geographic locations. An adequate sanctions compliance program will often include the use of counterparty "screening" tools (which compare counterparty information, including ultimate beneficial owners, against the SDN List and other relevant restricted party lists) as well as procedures for escalating transactions that pose an unacceptable risk of violating applicable sanctions. Screening protocols should be calibrated according to risk profile as well, including use of "fuzzy logic" algorithms. For some targets, reasonable sanctions compliance measures should include Internet Protocol address-based geo-blocking to prevent persons in sanctioned jurisdictions from accessing a company's online platform or products.

2. Dealings with Russia, Belarus, and Assessing Diversion Risk

Since Russia's 2022 full-scale invasion of Ukraine, the United States, in coordination with its allies and partners, has imposed a wide range of restrictions on trade with Russia and Belarus. For example, the United States has prohibited new investment in Russia, the importation into the United States of energy products from Russia, and the exportation of any military or dual-use products to Russia. In addition, OFAC has designated thousands of Russian persons and entities, including Russian oligarchs and family members, and imposed severe restrictions on dealings with Russia's banking, financial, energy, and military-industrial sector. OFAC has prohibited the provision of certain professional services, to persons located in Russia, including accounting, trust and corporate formation, management consulting, quantum computing, architecture, engineering, certain maritime transportation-related services, and IT services, among others. The Department of Commerce's Bureau of Industry and Security ("BIS") has imposed stringent export controls targeting Russia and Belarus, which cover a wide range of industrial and commercial items. In some cases, these restrictions extend to products made outside of the United States that depend upon U.S.-origin software, technology, or tools. As such, any business involving Russia and Belarus, directly or indirectly, can pose substantial international trade-related risks—especially if the target maintains a Russian subsidiary or branch office.

U.S. authorities have been particularly focused on diversion risk and efforts by companies to detect and prevent the illicit transfer of goods to restricted destinations via intermediaries and shell companies. More broadly, acquiring a target that is based in a jurisdiction that has not adopted export controls similar to those maintained in G7 states can carry elevated risk of unlawful diversion in violation of applicable sanctions and export controls. While virtually every industry is potentially at risk, the United States and its partners have issued advisories identifying high priority items that Russia is seeking to support its war effort and high-risk industries, for which trade with Russia is severely curtailed. Buyers should be on the lookout for trading patterns of a target that show a substantial shift in trade away from Russia to identified diversion points, or sudden spikes in sales to higher risk jurisdictions.

3. Export Controls

Many targets, including targets that are not traditional "manufacturers" (such as many producers of software), will also carry compliance obligations under export controls set forth in the Export Administration Regulations ("EAR"). Export controls are used by the United States and other nations to restrict the export of items that would contribute to the military potential of adversary countries or to restrict the export of items necessary to further foreign policy objectives and uphold treaty obligations. U.S. export controls have a broad extraterritorial reach, since the obligation to comply with requirements follows U.S. items wherever they are located and, in some instances, extends to foreign-made products that rely upon U.S.-origin technology, software, or tools. Export control requirements can apply based on the technical parameters and performance capabilities of an item or based upon the intended destination, end user, or end use. In some circumstances, the release of technology to a foreign national may require an export license as a "deemed export" to the country of residence of the recipient of the information.

Export control risks are most commonly presented in acquisitions of target companies that produce items with potential defense applications (i.e., "dual-use" items). These targets oftentimes operate in the aerospace, software, connected devices, and specialized and high-tech manufacturing industries. Of special relevance to targets operating in the software and high-tech industries, most encryption technology and software is subject to specialized export controls. Companies operating in these sectors, therefore, must maintain adequate policies and procedures in order to classify and, if applicable, fulfill the reporting requirements set forth in license exception ENC.

Export controls are a fast-developing area of international trade law. For example, on September 6, 2024, BIS published new regulations to control certain advanced and emerging technologies, including quantum computing, semiconductor manufacturing equipment, and additive manufacturing. These regulations represent an early step towards establishing a plurilateral export control regime to eventually replace the Wassenaar Arrangement, the legacy multilateral export control regime that includes Russia. BIS has also signaled its intent to increase penalties and enhance its enforcement efforts, in conjunction with international export control authorities. It is especially likely, therefore, that export controls-related due diligence obligations will expand during 2025.

4. CFIUS Risk

The Committee on Foreign Investment in the United States ("CFIUS") reviews foreign direct investments in U.S. businesses for national security risks. CFIUS examines certain transactions in which foreign entities gain control or make certain non-controlling investments in U.S. businesses. At the conclusion of its assessment, CFIUS may impose restrictions that address U.S. national security risks arising from those transactions. In 2018, the Foreign Investment Risk Review and Modernization Act expanded the scope of transactions subject to CFIUS review to include (i) certain non-controlling investments in U.S. businesses that implicate critical technology, critical infrastructure, or sensitive personal data of U.S. citizens and (ii) real estate located near sensitive U.S. military installations. CFIUS devotes particular attention to transactions with investors from adverse jurisdictions and transactions that implicate defense and other key supply chains or emerging technologies, such as AI.

The CFIUS review process, which typically begins with the transaction parties filing a mandatory or voluntary notice to CFIUS, can take 4-6 months or longer. Consequently, where an acquisition implicates CFIUS jurisdiction, deal timing should accommodate the time to submit a notification and receive clearance prior to closing. A completed CFIUS review grants "safe harbor," preventing future scrutiny from CFIUS. Without this safe harbor, CFIUS retains discretion to review and place conditions on transactions after they have been completed. There is no statute of limitations to CFIUS's ability to review closed transactions. In relatively rare circumstances, CFIUS may also recommend that the President block or unwind a transaction. CFIUS can assess monetary penalties on parties for failure to make a mandatory filing, for making material misstatements or omissions in a filing, or for failure to comply with a national security mitigation agreement.

5. Outbound Investment: "Reverse CFIUS" Risk

It is widely anticipated that the Department of the Treasury will promulgate "reverse CFIUS" outbound investment regulations during the next year. Currently, these regulations are expected to target investments made by U.S. persons in China, Hong Kong, or Macau and involving certain categories of technologies, including the development and production of semiconductors and microelectronics, quantum information technologies, and artificial intelligence systems. Proposed rules would impose recordkeeping and notification requirements on U.S.-person investors. Additionally, certain investments in advanced critical technologies may be prohibited. Diligence obligations during acquisitions will likely mirror those under current CFIUS regulations to identify transactions within the scope of the outbound investment regime.

6. Forced Labor and Importation Concerns

Some targets will present risks under the Uighur Forced Labor Prevention Act ("UFLPA"). The UFLPA presumptively bars from entry into the United States all products that are manufactured in China's Xinjiang Uyghur Autonomous Region or produced by a list of entities that have been designated by the interagency Forced Labor Enforcement Task Force ("FLETF"), unless the importer can present "clear and convincing" evidence that the product has not been tainted by the use of forced labor. U.S. Customs and Border Protection ("CBP"), which enforces the UFLPA, has been remarkably aggressive in enforcing these provisions. The UFLPA does not contain a *de minimis* exception, and CBP has barred shipments from entry into the United States where the goods contained under 1% of Xinjiang-origin content by value.

Accordingly, in addition to reviewing the target's documentation and conducting interviews with management, it may be necessary in some cases to use business intelligence platforms to "screen" targets and their counterparties for risks related to forced labor in the supply chain. Notably, owing to the absence of a *de minimis* exception, the UFLPA authorizes CBP to detain shipments that are not themselves manufactured in Xinjiang but contain inputs that originate, in whole or in part, in Xinjiang. As such, even targets that depend on imports from third countries, such as Vietnam, may present elevated risk of violating the UFLPA depending on the products involved.

7. Defense Sector Controls

There are unique considerations for targets operating in the defense sector, even if the target only handles defense-related items as a minority of its sales. In particular, the International Traffic in Arms Regulations ("ITAR") apply to defense articles, defense services, and related technology. The ITAR, like the EAR, "follow the item" and therefore have broad extraterritorial application. Under the ITAR, persons engaged in the business of manufacturing, exporting or temporarily importing defense articles, or furnishing defense services, are required to register with the Department of State's Directorate of Defense Trade Controls ("DDTC"). When a registered target is acquired, the target and the buyer are required to notify DDTC within five days of the closing. Where a buyer is a non-U.S. person, the buyer and target must submit a notice to DDTC at least 60 days before closing. These requirements apply even if the transaction is an acquisition of assets or a sale in the course of bankruptcy. A transaction that involves an ITAR registrant that occurs in a multi-step process could trigger multiple notifications. In addition to

registration, any export licenses that the target holds authorizing it to send defense articles outside of the United States must be requested to transfer to the new parent entity. It is essential that deal timelines accommodate registration, notification, and transfer requirements, as failure to do so could result in a disruption of business activities.

8. Managing Legacy International Trade Issues

If a target company has failed to adhere to relevant international trade controls, post-closing remediation may be necessary, including the possibility of self-disclosure to relevant government agencies. Under enforcement policies of the U.S. Department of Justice's National Security Division and the U.S. Department of Commerce, the prompt self-disclosure of a target company's apparent violations of sanctions and export control laws that occurred prior to acquisition may be eligible for significant mitigation credit. Conversely, a target company that has made serial self-disclosures may have systemic compliance issues, which may result in significant penalties for the buyer. In addition, compliance commitments and consent agreement terms may apply to buyers and related entities, even following acquisition.

Our attorneys are leading industry experts, and we regularly advise on international trade matters on behalf of the world's largest companies. We efficiently identify the costs and resources needed to implement post-acquisition remediation and assist in integrating the international trade practices of target companies into buyers' global organizations. We also help manage target companies' pre-existing compliance gaps and provide holistic assessments on the impacts of such events on the transaction or the buyer's business.

The following Gibson Dunn lawyers prepared this update: Adam M. Smith, Christopher Timura, Stephenie Gosnell Handler, Robert Little, Saee Muzumdar, George Sampas, Samantha Sewall, Michelle Weinbaum, and Zach Kosbie.

Gibson Dunn's lawyers are available to assist in addressing any questions you may have regarding these developments. For further information, please contact the Gibson Dunn lawyer with whom you usually work, the authors, or any leader or member of the firm's Mergers and Acquisitions, Private Equity, or International Trade practice groups:

International Trade:
Adam M. Smith – Washington, D.C. (+1 202.887.3547, asmith@gibsondunn.com)
Stephenie Gosnell Handler – Washington, D.C. (+1 202.955.8510, shandler@gibsondunn.com)
Christopher T. Timura – Washington, D.C. (+1 202.887.3690, ctimura@gibsondunn.com)
Samantha Sewall – Washington, D.C. (+1 202.887.3509, ssewall@gibsondunn.com)
Michelle A. Weinbaum – Washington, D.C. (+1 202.955.8274, mweinbaum@gibsondunn.com)

Mergers and Acquisitions:
Robert B. Little – Dallas (+1 214.698.3260, rlittle@gibsondunn.com)
Saee Muzumdar – New York (+1 212.351.3966, smuzumdar@gibsondunn.com)
George Sampas – New York (+1 212.351.6300, gsampas@gibsondunn.com)

Private Equity:
Richard J. Birns – New York (+1 212.351.4032, rbirns@gibsondunn.com)
Ari Lanin – Los Angeles (+1 310.552.8581, alanin@gibsondunn.com)
Michael Piazza – Houston (+1 346.718.6670, mpiazza@gibsondunn.com)
John M. Pollack – New York (+1 212.351.3903, jpollack@gibsondunn.com)