Strategic Perspectives

Wolters Kluwer

February 16, 2022

Russia-Ukraine: Potential sanctions and SEC disclosure issues

By Mark S. Nelson, J.D., and John M. Pachkowski, J.D.

Although continuing diplomatic efforts seek to avoid a Russian invasion of Ukraine, attorneys advising companies doing business in the region are listening to the aggressive rhetoric and considering the impact on their clients. Here we consider the sanctions that could be imposed against individuals and entities operating in the region and what companies should be considering as events unfold. Counsel for these companies may need to update SEC disclosures related to risk factors or take into account specific considerations related to banks, oil and gas businesses, or M&A activity. Cybersecurity is another concern, with the Cybersecurity & Infrastructure Security Agency warning companies to stay on alert for intrusions.

The Biden Administration has stated on a number of occasions that invading Ukraine would result in "swift and severe" costs to Russia in the form of economic sanctions (remarks here and here). If sanctions were to be imposed on Russia in response to its invasion of Ukraine, National Security Advisor Jake Sullivan said at a January 13, 2022, press briefing, that they are approaching it "with a 'start high, stay high' mentality, not a graduated application of these sanctions."

"From all angles." During a January 31, 2022, White House Press Briefing, Press Secretary Jen Psaki further elaborated on the contours of the Administration's planned sanctions against Russia, saying that specific sanctions have been developed for both Russian elites and their family members if Russia invades Ukraine. She added, "Many of these individuals are particularly vulnerable targets because of their deep and financial ties with the West, meaning they would be hurt by sanctions that are tying them to Western financial systems." Psaki concluded, "I would also note that this is just one piece of our effort to hit Russia from all angles."

OFAC sanctions program. The most likely scenario for sanctions to be imposed upon Russia would be an expansion of the Ukraine/Russia-related sanctions program implemented by the Office of Foreign Assets Control in 2014. That sanctions program was created in response to a national emergency, declared by President Obama in Executive Order 13660, to deal with the threat posed by the actions and policies of certain persons who had undermined democratic processes and institutions in Ukraine; threatened the peace, security, stability, sovereignty, and territorial integrity of Ukraine; and contributed to the misappropriation of Ukraine's assets. In further response to the actions and policies of the Government of the Russian Federation, including the purported annexation of the Crimea region of Ukraine, President Obama issued three subsequent Executive Orders—13661, 13662, and 13685—that expanded the scope of the national emergency declared in Executive Order 13660.

The OFAC program, codified at 31 CFR Part 589, has imposed sanctions based on three broad categories: 1) blocking sanctions against individuals and entities designated pursuant to Executive Orders 13660, 13661, 13662, or 13685 and listed on the List of Specially Designated Nationals and Blocked Persons (SDN List); 2) sectoral sanctions against entities operating in sectors of the Russian economy identified by the Secretary of the Treasury pursuant to Executive Order 13662 and listed on the Sectoral Sanctions Identification List (SSI List); and 3) a ban on investment and prohibition on the exportation or importation of goods, technology, or services to or from the Crimea region of Ukraine.

Congressional action. Besides expanding upon the OFAC sanctions, Senator Robert Menendez (D-NJ) has introduced the Defending Ukraine Sovereignty Act of 2022, on January 12, 2022, as S. 3488. The legislation, if enacted, would require the President to periodically determine whether Russia's government is significantly escalating hostilities in or against Ukraine and whether such an escalation has the aim or effect of undermining Ukraine's government or interfering with Ukraine's sovereignty or territorial integrity. If the President determines that Russia's government has engaged in such escalation, the President must impose sanctions on: 1) certain government officials, including Russia's president and prime minister; 2) certain Russian financial institutions; 3) entities involved in certain transactions involving Russian debt; 4) entities (and corporate officers of such entities) involved in constructing or operating Russia's Nord Stream 2 natural gas pipeline; and 5) certain entities involved in Russian resource extraction industries.

SEC disclosures. U.S. companies with material business in Russia or Ukraine may elect to update existing SEC disclosures to reflect the risks of doing business in these countries if geopolitical tensions there evolve into open hostilities. Russia's dependence on oil & gas exports may significantly impact businesses that interact with that segment of the Russian economy in the event that open hostilities lead to the imposition by the U.S. and other countries of economic sanctions and to the extent open hostilities between Russia and Ukraine may lead to disruptions in oil & gas supplies or related projects such as the Nord Stream 2 pipeline that may have impacts in Russia, Ukraine, and Europe more generally. Likewise, the banking sector could be significantly impacted if economic sanctions are imposed on Russia. Several SEC disclosure requirements may apply.

- ***Risk factors***—Item 105 of Regulation S-K requires companies to, where appropriate, provide risk factors that explain the material factors that make an investment in the company or in a particular offering speculative or risky. Item 105 discourages the use of generic risk factors that state risks applicable to any company or offering, but also provides that, if such generic risk factors are included in SEC filings, they should be grouped together at the end of the risk factor section under the heading "General Risk Factors." Moreover, if the risk factor section is longer than 15 pages, the company must include an up to two-page, bulleted summary of the principal risks to the company or the offering in the forepart of the prospectus or annual report.

- ***MD&A trends***—Item 303 of Regulation S-K requires a company to include in its Forms 10-Q and 10-K a narrative disclosure that explains the nature of its business and results of operations in the words of its mangers. Among the several things a company must discuss are those contained

in Item 303(b)(2) regarding trends in the company's business. Specifically, a company must: (i) describe any unusual or infrequent events or transactions that materially affect its reported income from operations and the extent of that affect on income; (ii) describe known trends or uncertainties that have or are reasonably likely to have a material favorable or unfavorable impact on net sales or reserves or income from continuing operations; and (iii) if its statement of comprehensive income presents period-to-period changes in net sales or revenue, the company may need to also describe the extent to which these changes are attributable to changes in volume/amount of goods or services sold. The SEC's latest amendments to Item 303 became effective February 10, 2021, with compliance required for a registrant's first fiscal year ending on or after August 9, 2021. (See, Management's Discussion and Analysis, Selected Financial Data, and Supplementary Financial Information, Release No. 33–10890, November 19, 2020, 86 F.R. 2080, January 11, 2021).

Item 302(b) of Regulation S-K also requires companies that engage in oil & gas producing activities, as defined in Rule 4-10(a)(16) of Regulation S-X, to present the information specified in FASB ASC 932 if those activities are significant in that they would meet one or more of the tests contained in FASB ASC 932-235. The Commission's proposal to amend Item 303 of Regulation S-K had proposed to eliminate Item 302(b), but the final rules retained Item 302(b) because FASB had not yet finalized its applicable revisions to GAAP. The Commission indicated that the elimination of Item 302(b) may be considered in a future rulemaking. (See, Management's Discussion and Analysis, Selected Financial Data, and Supplementary Financial Information, Release No. 33–10890, November 19, 2020, 86 F.R. 2080, 2087, January 11, 2021).

Moreover, in the case of companies in engaged in the oil & gas business, guidance included as part of the 2008 reforms of Regulation S-K listed a series of items that such companies may need to address in their MD&A. One of those items is the geopolitical risks that apply to material concentrations of reserves. (See, Modernization of Oil and Gas Reporting, Release No. 33–8995, December 31, 2008, 74 F.R. 2158, 2178-2179, January 14, 2009).

- ***Oil & gas industry disclosures***—The Russian economy is heavily dependent on its oil & gas industry. Companies engaged in the oil & gas industry in Russia may need to include specific disclosures about reserves, production, and drilling under federal securities regulations. Items 1201, et. seq., of Regulation S-K provide details on what must be disclosed and when that information must be disclosed. In general, material oil & gas producing activities must be disclosed, but limited partnerships and joint ventures that engage in certain activities may not have to include such disclosures. When disclosures are required to be "by geographic area" the disclosure must provide information by individual country, by groups of countries within a continent, or by continent.

- ***Resource extraction issuers***—Following Congressional disapproval of the SEC's original resource extraction issuer rules under the Congressional Review Act, the Commission reissued similar rules in 2020. The resource extraction issuer rules require companies engaged in extractive industries to disclose information relating to any payment made by the resource extraction issuer, a subsidiary of the resource extraction issuer, or an entity under the control of the resource extraction issuer to a foreign government or the federal government for the purpose of the commercial development of oil, natural gas, or minerals.

The reissued resource extraction issuer regulations became effective on March 16, 2021, but the Commission also adopted a two-year transition period for compliance. As a result, a resource extraction issuer must comply with Exchange Act Rule 13q-1 and Form SD no earlier than two years after the effective date of the final rules. The final rules provide the following example: "if the rules were to become effective on March 1, 2021, the compliance date for an issuer with a December 31 fiscal year-end would be Monday, September 30, 2024 (i.e., 270 days after its fiscal year end of December 31, 2023)."

Questions may arise regarding the enforceability of the reissued rules because the Congressional Review Act provides that an agency may not reissue rules that are in substantially the same form as the disapproved rules without new Congressional authority. To date, no such new legislative authority has been enacted into law, although legislation has been proposed to accomplish that objective. (See, e.g., a discussion draft of the Oil and Minerals Corruption Prevention Act, proposed by Rep. Brad Sherman (D-Calif)).

The Commission's December 2020 re-write noted that the Congressional disapproval resolution did not alter the original Congressional mandate and, thus, the Commission had an obligation to issue new rules. However, to avoid issuing rules in substantially the same form as the disapproved rules, the Commission focused on revising two items over which it believed it had discretion: (1) rules for the publication of issuers' payment disclosures as compared to anonymization; and (2) the "relative granularity" regarding how "project" is defined. The latest version of the regulation also includes conditional exemptions regarding conflicts of law, conflicts with pre-existing contracts, and emerging growth companies and smaller reporting companies (See, Disclosure of Payments by Resource Extraction Issuers, Release No. 34–90679, December 16, 2020, 86 F.R. 4662, January 15, 2021).

Disclosure of payments by resource extraction issuers remains on the Commission's Fall 2021 Unified Agenda of Regulatory and Deregulatory Actions.

- ***Bank disclosures***—Under Item 1401(d) of Regulation S-K, bank holding companies must disclose foreign financial activities only if the information to be presented meets the thresholds for separate disclosure contained in Rule 9-05 of Regulation S-X. Under Rule 9-05 of Regulation S-X, a BHC must provide separate disclosure of its foreign activities for each period in which either its (1) assets, or (2) revenue, or (3) income/loss before income tax expense, or (4) net income/loss, each associated with its foreign activities, was greater than 10 percent of the corresponding amount in its related financial statements. Certain types of information must be presented separately for each significant geographic area and in the aggregate for non-significant geographic areas. Rule 9-05 defines "foreign activities" to mean loans and other revenue producing assets and transactions in which the debtor or customer, whether an affiliated or unaffiliated person, is domiciled outside the United States. Rule 9-05 defines "significant geographic area" to mean an area in which assets or revenue or income before income tax or net income exceed 10 percent of the comparable amount as reported in the financial statements.

Instruction 5. to Item 1402 of Regulation S-K states that if disclosure under Item 1401(d) is required, the information required by Item 1402 must be further segmented between domestic and foreign activities for each significant category of assets and liabilities. Moreover, a BHC must, for each period, present separately, on the basis of averages, the percent of total assets and total liabilities attributable to foreign activities.

The Instructions to Item 1405 of Regulation S-K provide that certain information regarding allowances for credit losses need not be disclosed if the BHC is a foreign private issuer that follows IFRS.

Several provisions regarding deposits contained in Item 1406 of Regulation S-K may apply to a BHC's foreign activities. For one, Item 1406(c) states that, if material, a BHC must disclose separately the aggregate amount of deposits by foreign depositors in domestic offices but need not identify the depositors' nationality. Under Item 1406(e), a foreign banking or savings and loan registrant must disclose the definition of uninsured deposits appropriate for its country of domicile. Item 1406(f)(2) requires that a BHC state the amounts of otherwise uninsured timed deposits by the time remaining until maturity as specified by Item 1406; the disclosure would include non-U.S. time deposits in excess of any country-specific insurance fund limit.

Revisions to the Regulation S-K banking disclosure requirements became effective November 16, 2020, with a compliance date of December 15, 2021, also known as the mandatory compliance date. Prior to the mandatory compliance date, the Commission retained, and banks were advised to follow, the Securities Act and Exchange Act Guide 3 titled "Statistical Disclosure by Bank Holding Companies." The two Guide 3 documents will be removed and reserved as of January 1, 2023. (See, Update of Statistical Disclosures for Bank and Savings and Loan Registrants, Release No. 33–10835, September 11, 2020, 85 F.R. 66108, October 16, 2020).

Forms 8-K and 6-K. Companies subject to Exchange Act reporting requirements use Form 8-K to report unscheduled material events. A company generally must file or furnish (as appropriate) Form 8-K within four business days after a reportable event has occurred, subject to some adjustments in timing for weekends and holidays, and subject to the requirements for Regulation FD disclosures (Rule 100(a) of Regulation FD distinguishes between simultaneous and prompt disclosures depending on whether the Regulation FD disclosure was intentional or non-intentional, respectively) and "other" disclosures (discussed below). Some of the more common Items within Form 8-K can apply generically to almost any business, while some of them may have greater relevance to companies engaged in banking or the extractive industries:

Items 1.01 and 1.02—Entry into/termination of a material definitive agreement.

Item 1.03—Bankruptcy or receivership.

Item 2.01—Completion of acquisition or disposition of assets.

Item 2.02. Results of operations and financial condition.

Items 2.03 and 2.04. Creation of/triggering events related to a direct financial obligation or an obligation under an off-balance sheet arrangement of a registrant.

Item 2.06. Material impairments.

Item 5.05. Amendments to the registrant's code of ethics, or waiver of a provision of the code of ethics.

Items 6.01 to 6.06—Asset-backed securities.

Item 8.01—Other events. Companies may disclose on Form 8-K other events that are not explicitly required to be disclosed on such form but which the company deems to be important to holders of its securities.

A foreign private issuer that is required to furnish reports under Exchange Act Rules 13a-16 or 15d-16 would file Form 6-K, which is similar to Form 8-K.

SEC staff OFAC comment letters. As part of the SEC's filing review process, SEC staff occasionally issue comments to companies regarding compliance with Office of Foreign Asset Control sanctions regimes. These OFAC-themed staff comments letters often focus on the potential that a company will suffer reputational harm from violations of the various sanctions regimes overseen by OFAC.

A somewhat recent example of such a dialogue involved PayPal Holdings, Inc., in which SEC staff asked PayPal to further explain its settlement with OFAC regarding sanctions violations and to clarify its disclosures regarding a news media report that PayPal had received related DOJ subpoenas. PayPal's initial response explained that the transactions flagged by OFAC had involved payments processed by PayPal or its subsidiaries that, due to human error, had evaded PayPal's screening system. PayPal also said that because it was unsure whether OFAC would consider the transactions to be violations, the company could not state what potential reputational harm could result from the transactions. PayPal also indicated that the DOJ subpoenas reported by media outlets may have been previously disclosed in its earlier Forms 10-K and 10-Q in relation to an AML issue rather than potential sanctions violations.

An SEC follow-up letter reiterated the staff's prior request for the names of the countries involved. PayPal responded that the countries included North Korea, Iran, Sudan, and Syria. PayPal also said the transactions did not involve the governments of those countries, were negligible and de minimis with respect to total volume and dollar value, and that the transactions accounted for only a small portion of PayPal's global revenue from its transaction processing business. PayPal also stated that it has policies and procedures to prevent such transactions from being processed, denies account registration to prohibited persons and entities in sanctioned countries, blocks access to PayPal websites

by sanctioned countries, and blocks IP addresses known to be associated with persons in sanctioned countries. Overall, PayPal said the transactions at issue were not material to a reasonable investor, although the company noted uncertainty about what if any, action OFAC may take.

The SEC staff's dialogue with ING Groep N.V. also provides an earlier example of OFAC-themed comments in the context of a traditional bank. There, the SEC staff inquired regarding an alleged effort by several of the company's global offices to hide transactions with Cuba and Iran that were banned under federal law. ING eventually agreed to abide by deferred prosecution agreements with federal and New York law enforcement agencies, requiring the company to pay a $619 million penalty. ING's related settlement with OFAC was the largest settlement of its kind at the time. The SEC's comment letters emphasized the potential for ING to suffer reputational harm.

Cybersecurity. If geopolitical tensions between Russia and Ukraine evolve into open hostilities, the U.S. and its European allies will likely impose strong sanctions against Russia. It is plausible that Russia could retaliate against nation states or businesses operating in nation states that support sanctions against Russia and that that retaliation could take the form of government-sanctioned cyberattacks or cyberattacks perpetrated by criminal groups or other state or non-state actors who sympathize with Russia. U.S. businesses should be alert to the possibility of cyberattacks associated with any developments regarding Russia and Ukraine.

The Commission's 2018 interpretation related to cybersecurity disclosures updated its prior guidance that was issued in 2011 (CF Disclosure Guidance: Topic No. 2) but retained the emphasis on materiality while adding new guidance on the need for companies to have cybersecurity policies and procedures and for companies to avoid scenarios that could involve insider trading related to cyber incidents. The Commission reiterated that a company need not make disclosures that would provide hackers with a "roadmap" to the company's vulnerabilities, but the company should disclose cybersecurity risks and incidents that are material and discuss the related financial, legal, or reputational consequences. Cyber disclosures can evolve over time as the facts of a cyber incident become known and, thus, companies may need to correct earlier disclosures. (See, Commission Statement and Guidance on Public Company Cybersecurity Disclosures, Release No. 33–10459, February 21, 2018, 83 F.R. 8166, February 26, 2018). The Commission recently proposed to extend cybersecurity regulations to investment advisers, registered investment companies, and business development companies.

Moreover, the Cybersecurity & Infrastructure Security Agency (CISA) has issued an alert urging U.S. businesses to raise their state of alert in the event that open hostilities occur between Russia and Ukraine. CISA suggested that firms working with organizations in Ukraine take additional steps to monitor, inspect, and isolate online traffic with those organizations, including a review of access controls. "While there are not currently any specific credible threats to the U.S. homeland, we are mindful of the potential for the Russian government to consider escalating its destabilizing actions in ways that may impact others outside of Ukraine," said the alert. According to the alert, Russia has employed cyber to project force around the globe during the past decade, including via previous operations in Ukraine.

CFIUS merger reviews. The Committee on Foreign Investment in the United States (CFIUS), housed within the Treasury Department, reviews transactions involving foreign investment in the U.S and real estate transactions by foreign persons for the purpose of understanding how those transactions may impact the national security of the U.S. Through CFIUS reforms enacted via the Foreign Investment Risk Review Modernization Act (FIRRMA) of 2018, Congress has continued to sharpen its focus on limiting the influence of Chinese companies in U.S. markets, especially those companies with ties to China's Communist government, as a way of blunting the growing economic and military rivalry between the U.S. and China. However, CFIUS reviews extend to transactions with businesses in other countries. Transactions in which Russian or Ukrainian companies make investments in the U.S. could receive CFIUS scrutiny.

FCPA issues. The Foreign Corrupt Practices Act (FCPA), with many of its operative provisions contained in portions of the Exchange Act, sets forth two related approaches to corrupt business practices by focusing on bribery and accounting provisions. The accounting provisions are further subdivided into provisions requiring companies to maintain books and records and internal controls. Beyond these basics, FCPA practitioners also should be aware of several recent developments regarding the definition of "foreign official" and the use of disgorgement in FCPA actions.

First, the FCPA can apply broadly as at least one recent court opinion demonstrates. The FCPA, at 15 U.S.C. §78dd-2(h)(2)(A), defines "foreign official" to mean "any officer or employee of a foreign government or any department, agency, or instrumentality thereof, or of a public international organization, or any person acting in an official capacity for or on behalf of any such government or department, agency, or instrumentality, or for or on behalf of any such public international organization." The word "instrumentality," however, is undefined. The Eleventh Circuit in *U.S. v. Esquenazi* (2014) (cert. den'd), defined "instrumentality" to mean "an entity controlled by the government of a foreign country that performs a function the controlling government treats as its own."

The Eleventh Circuit noted that the judicially-created explanation of "instrumentality" requires a factual evaluation of what it means to "control" and what it means for a function to be "a function the government treats as its own." The court said "control" can be shown by examining: (1) the foreign government's formal designation of the entity; (2) whether the government has a majority interest in the entity; (3) the government's ability to hire and fire the entity's principals; (4) the extent to which the entity's profits, if any, go directly into the governmental fisc or the extent to which the government funds the entity if it fails to break even; and (5) the length of time these indicia have existed.

Likewise, "a function the government treats as its own" can be demonstrated by showing: (1) whether the entity has a monopoly over the function it exists to carry out; (2) whether the government subsidizes the costs associated with the entity providing services; (3) whether the entity provides services to the public at large in the foreign country; and (4) whether the public and the government of that foreign country generally perceive the entity to be performing a governmental function.

Second, the conference report for the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021 (NDAA) (H.R. 6395), secured the SEC's right to seek, and the authority of federal courts to order, disgorgement in securities enforcement matters. The SEC's disgorgement authority had been challenged in *Kokesh v. SEC* (2017), in which the Supreme Court held that disgorgement is a "penalty" subject to the general federal five-year limitations period. The NDAA retained the five year limitation period for many such violations but added a new 10-year limitations period for scienter-based violations. Although the SEC now has clearer disgorgement authorities, a subsequent Supreme Court opinion in *Liu v. SEC* (2020) held that a disgorgement award that does not exceed a wrongdoer's net profits and is awarded for victims is permissible equitable relief, thus stating some key limiting principles for the SEC when it seeks disgorgement. The *Liu* opinion, however, stated two additional limiting principles on the SEC's disgorgement authorities, which also can apply in the FCPA setting: (1) courts must deduct legitimate expenses before ordering disgorgement; and (2) joint and several liability can be imposed where, as the common law allowed, partners have engaged in concerted wrongdoing.

It is unclear if the FCPA would have an immediate impact in the event that tensions between Russia and Ukraine were to become open hostilities because FCPA cases can take months or years to be fully investigated before any charges are brought. Nevertheless, any U.S. business operating in Russia or Ukraine should have in place appropriate internal controls and written policies and procedures to reduce the risk for potential FCPA violations.

Looking ahead. As the world awaits either a diplomatic resolution or the onset of hostilities between Russia and Ukraine, companies subject to U.S. regulations will continue to update their contingency plans for the potential that events overseas may significantly impact their business operations. In the event of hostilities between Russia and Ukraine, strong economic sanctions imposed by the U.S. and its European allies on Russia will likely be at the vanguard of the world's reaction to Russian aggression towards Ukraine. Securities disclosure obligations may soon follow for many companies, depending on the evolution of events. However, the potential for Russian retaliation in response to sanctions may involve cybersecurity actions that could impact U.S. businesses far beyond the banking and oil & gas sectors of the economy likely to be most impacted by open hostilities between Russia and Ukraine. As a result, all U.S. businesses have been warned by government regulators to raise their level of alert for potential cyberattacks.