CLEARY GOTTLIEB

Chase D. Kaniecki is a partner and Samuel H. Chang is an associate at Cleary Gottlieb Steen & Hamilton LLP. Mr Kaniecki can be contacted on +1 (202) 974 1792 or by email: ckaniecki@cgsh.com. Mr Chang can be contacted on +1 (202) 974 1816 or by email: sachang@cgsh.com.

EXPERT BRIEFING ARTICLE August 2022

Sanctions compliance and contingency planning: lessons from the conflict in Ukraine

BY CHASE D. KANIECKI AND SAMUEL H. CHANG

The Western response to the ongoing conflict in Ukraine has brought into sharp focus not only the central role of economic sanctions in modern geopolitical conflicts, but also the speed at which sanctions – and the mere threat of sanctions – can disrupt markets, industries and commercial operations.

In such environments, company executives and boards may be called on to make consequential decisions based on technical rules under significant uncertainty and time constraints. As a number of companies have learned during the conflict in Ukraine, having appropriate compliance procedures and advanced contingency planning can be invaluable to streamline such decision making, minimise the risk of sanctions violations and mitigate operational disruptions.

While the scope and rigour of such preparation will depend on the circumstances and risk profile of each company, this article describes general principles for consideration.

Compliance framework

Although unprecedented in a number of ways, the majority of recent US, European Union (EU) and UK sanctions against Russia have fit into existing regulatory frameworks and resembled regulatory provisions from prior sanctions programmes. Thus, during the initial stages of the conflict in Ukraine, companies with established sanctions compliance programmes (SCPs) had a significant advantage over companies that were unfamiliar with general sanctions compliance requirements. As a number of businesses found, it is easier to adapt and tailor existing compliance procedures to new restrictions than to draft and implement a new SCP in the midst of a crisis.

Organisational structure. As the US Department of the Treasury, Office of Foreign Assets Control (OFAC) has stated in guidance on compliance expectations, there is no such thing as a 'one size fits

all' SCP. Instead, companies should tailor their SCPs according to their industry, counterparty and company risk profiles. At a high level, however, SCPs should designate an officer (e.g., a chief compliance officer or sanctions compliance officer) with responsibility for day to day sanctions compliance and general contingency planning. Such compliance officers are most effective when they have decision-making authority and report directly to senior leadership. The designated officer or other members of the sanctions compliance team often benefit from being integrated with other groups within the company – including the risk, legal, accounting or finance teams, as well as certain business units. Such relationships can facilitate close coordination during a crisis and alert the compliance team to changes in the company's risk profile and prevent and identify potential violations.

Screening procedures. While any compliance programme will include a number of components, the core of an SCP are effectively tailored screening procedures to verify whether a company's counterparties or activities are subject to sanctions – for example, as a result of being designated on a sanctions list, owned or controlled by a designated party, or located in a sanctioned jurisdiction. Because OFAC and, as of March 2022, UK sanctions operate under strict liability, ignorance to prohibited dealings with sanctioned parties is no defence to civil enforcement actions. Companies often adopt a risk-based approach to screening and may conduct more thorough ownership and related due diligence on counterparties or business in higher risk jurisdictions.

Such screening procedures – both for new customers as well as periodic reviews of existing relationships – provide situational awareness on sanctions risks and can be deployed for risk assessments and responding to rapidly changing sanctions landscapes. For example, in a matter of weeks during the conflict in Ukraine, OFAC alone added over 1000 new parties to sanctions lists, in addition to imposing new territory- and activity-based restrictions. Effective screening procedures are thus critical for staying up to date with the escalation of sanctions, particularly when multiple jurisdictions may issue sanctions with subtle differences across regimes.

Risk assessment

Although sanctions can be unpredictable in nature and generally take immediate effect upon their imposition, companies can take steps to prepare for the collateral impacts of sanctions. In some instances, advance indicators – statements by public officials, proposed legislation or news reports of geopolitical flashpoints – may assist companies anticipate and mitigate the impact of future sanctions. For example, although the speed and breadth of western sanctions against Russia surprised many market actors, a draft US Senate sanctions bill, introduced over a month before the present conflict in Ukraine, offered a roadmap of proposed sanctions, almost all of which were ultimately issued by the Biden administration.

Before a company can properly prepare a response plan, however, it must first identify and evaluate its exposure to sanctions risks. As with SCPs, an effective sanctions risk assessment may be integrated with a broader assessment of related risks (such as anti-money laundering, anticorruption, supply chain integrity or cyber security) and take a number of forms, but it should incorporate some basic principles and be periodically refreshed.

Identify key touchpoints. Companies should identify any key touchpoints (direct or indirect) to external parties – for example, with suppliers, distributors, service providers, financial institutions, insurers, business partners or government agencies. For each key relationship identified, companies may consider verifying the relevant counterparty's identity, place of residence or incorporation, ownership structure, and, where appropriate, the counterparty's banks, supply chains, customer base, geographic exposure and key personnel. In light of the increasing imposition of export controls in parallel with sanctions – also demonstrated in the conflict in Ukraine – companies engaged in the manufacture or sale of goods may also consider identifying the relevant country of origin and export control classifications of their products and key inputs, as well as their consignees and end users.

Companies with robust sanctions and export compliance procedures may already have much of the above information available and would simply need to refresh their records. However, those with more limited compliance resources may consider prioritising mission-critical businesses and operations or rely on information gathered from planning for non-sanctions contingencies.

Anticipate potential sanctions. Companies also should outline potential sanctions scenarios based on any relevant regions, industries, products, activities or parties that are or may become the subject of future sanctions. Consultation with sanctions specialists is particularly crucial at this stage, as such scenarios will likely be informed by historical and existing sanctions. While certain types of potential sanctions restrictions or targets may be quickly determined to be implausible or irrelevant, it is generally best to begin with a broad approach, as indirect connections to potential sanctions risks may not be immediately apparent (e.g., transfer of items produced from US technology, indirect sales or access to data servers).

Companies should also consider potential retaliatory countermeasures, as a number of governments have established new, or significantly expanded existing, sanctions regimes in recent years. For example, Russia has sanctioned certain business executives, imposed capital controls, and threatened asset seizures and criminal prosecution for compliance with western sanctions. In addition, companies should be aware of potential conflict-of-laws issues when operating across multiple jurisdictions, particularly with respect to jurisdictions that have issued so-called blocking statutes prohibiting compliance with third-country sanctions.

Identify vulnerabilities. In addition, companies should identify vulnerabilities to their businesses, operations and investments. By synthesising the findings from the two preceding analyses, companies can evaluate the effect of potential sanctions scenarios on key external

touchpoints and, from there, prioritise the key sanctions contingencies based on their likelihood of occurrence and severity of impact.

Of particular relevance to this analysis are the jurisdictions to which a company, its affiliates and personnel are subject. Although sanctions laws only apply to parties acting within the jurisdiction of the relevant sanctions authority (e.g., as a result of location, nationality, residency, place of incorporation, or, in certain instances, ownership), such jurisdiction may be far reaching. For example, an Indian company is generally prohibited from processing a US dollar transaction involving a US-sanctioned party and a Mexican company may be prohibited from allowing an EU-national employee to participate in business with an offshore company controlled by an EU-sanctioned Russian oligarch.

Companies should also consider second-order effects of sanctions. For example, companies may consider compiling their contracts with key counterparties and analyse their rights and obligations under sanctions-related representations, covenants and force majeure clauses (all of which are frequently incongruent with requirements under sanctions laws), as well as choice-of-law and forum selection provisions, which may determine the applicability of contract-law doctrines of illegality, frustration or impossibility. Companies should also expect to encounter counterparties (particularly financial institutions), that – due to risk management, ethical or reputational concerns – may refuse to engage in dealings relating to sanctioned parties even when not prohibited by law.

Crisis response preparation

The specifics of a company's response plan – including, for example, sourcing from alternative counterparties, maintaining operations through a subsidiary, suspending operations or full divestment – will depend on the company's particular circumstances and risk tolerance. However, no company can plan for every contingency and even the best prepared companies faced a number of novel sanctions issues during the initial weeks of the conflict in Ukraine.

Companies should consider appointing a sanctions crisis response team both to implement contingency plans for anticipated sanctions and to manage a coordinated response to unanticipated sanctions. The team should have adequate resources and decision-making authority with minimal approval processes. Companies based in non-sanctioning jurisdictions that choose to continue operations with, for example, sanctioned parties or jurisdictions should impose a firewall for personnel who are nationals of the sanctioning jurisdiction and consider organising an internal 'clean team' – a group of employees who are not subject to the relevant jurisdiction – to independently deal with activities involving sanctioned parties or jurisdictions.

The increasing complexity of the sanctions landscape and speed at which new sanctions may be imposed can create a corporate crisis for unprepared companies. However, with some foresight, preparation and a sanctions contingency plan, companies may be better equipped to respond to new sanctions, avoid violations and minimise any disruptions to their businesses. ■