CORPORATE COUNSEL
An ALM Website
corpcounsel.com | September 10, 2019

A Guide for GCs Investigating Suspected Economic Sanctions and Export Control Violations

By Mario Mancuso, Sanjay Mullick, Anthony Rapa and Abigail Cotterill

On Friday evening, you get a call informing you that your company's German subsidiary may have shipped products to Iran. How do you confirm this allegation is true? Do you inform the board? Should you tell the government? You ask yourself, "What do I do next?"

When a company discovers that it may have committed a violation of economic sanctions or export control (ES/EC) laws, it needs to react swiftly and methodically. The following checklist provides guideposts for considering and conducting such investigations, with emphasis on features unique to ES/EC laws.

- **Assess the Information.**

The company must quickly assess the information's merit. An anecdotal comment is different from a report with a paper trail. Seek to establish the precise scope of the issue, how long it has been going on, and whether it is still occurring. This process may include confirmatory steps such as background conversations with the persons who discovered the potential violations and preliminary testing of ERP data for indicators of sales to sanctioned countries or prohibited end users or uses. Take care to establish privilege over the preliminary review through involvement of in-house and/or external counsel.

Peshkova/Shutterstock.com

- **Be Aware of the Context.**

The method by which information regarding a potential ES/EC violation surfaces can be relevant to the initial approach to response. It may have come to light in transaction diligence, during a routine compliance audit, or in response to a lender's questions regarding where the company does business. Alternatively, the trigger may have been an employee whistleblower or a query from the bank processing payment for one of the company's transactions. Work with the legal department or outside counsel to respond in accordance with applicable company protocols, protect confidentiality and privilege as possible, and ensure that there is no retaliation for reporting.

- **Contain the Problem.**

One of the most important first steps is to prevent additional violations from occurring. For example, implementation of "blocks" in an online drop-down menu to prevent customers from selecting certain countries (e.g., Iran) may stop additional shipments to those destinations. ES/EC violations that occur after discovery of a problem may be considered willful or intentional, increasing exposure to penalties.

• **Consider Voluntary Self-Disclosure.**

Another key early decision will be whether to self-report to the ES/EC regulators, namely the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC), the U.S. Department of Commerce's Bureau of Industry and Security (BIS), and the U.S. Department of State's Directorate of Defense Trade Controls (DDTC). It involves weighing several factors, including the probability that violations actually occurred, the likelihood that the government would find out about them independently, and the desire to have a clean slate, including being "exit ready" for future mergers and acquisitions. A particularly relevant consideration is that voluntary self-disclosures are afforded a fifty percent reduction in any penalties that may be imposed.

• **Secure Management Buy-In.**

Making a voluntary self-disclosure means notifying the government of the suspected violations fairly promptly, as letting time lapse can undermine voluntariness credit. It also means then carrying out a bona fide internal investigation, potentially including employee interviews, forensic review, and an analysis of up to five years of transaction data to check for ES/EC violations more broadly. In addition, it requires considering whether government authorizations may be necessary to engage in or continue certain activities. It is important to set the proper scope and obtain the necessary support, as the company must follow through and submit a report on what it commits to undertaking and the government will hold it accountable for those representations.

• **Develop a Work Plan.**

Upon deciding to proceed, it is advisable to design a guiding work plan. It should include technical work streams such as ERP searches for sanctioned countries, screening of counterparties against restricted lists and resolution of potential matches with restricted parties, and review of product export control classifications and potential license exceptions. It should also allot time to address the data privacy issues inherent in many cross-border transactional reviews, and incorporate strategic work streams such as identifying the root cause of potential violations, checking for the possibility that violations were intentional or willful, and adopting compliance enhancements. The company's actions likely will come under scrutiny from stakeholders such as its Board, auditors, investors, and lenders, and potentially the government.

• **Preserve Relevant Evidence.**

To safeguard the integrity of the investigation, at its outset steps must be taken to preserve relevant records and materials. Issue a hold notice to employees that is sufficiently broad to cover documents and communications relevant for ES/EC purposes, such as on sales and shipments, and on any prior interactions with government. Check for and suspend automatic deletion functions the company may have, e.g., for emails and other records stored on its servers. It will be counterproductive if the review is incomplete, or if the government forms the view relevant information has been lost, even inadvertently.

• **Initiate Appropriate Remediation.**

Even in an investigation's early stages, it is not too soon to commence remedial steps. Closing identified gaps, such as by making technical fixes to company systems and potentially integrating specialist third party providers, is a process that benefits from lead time. Ultimately, it will be necessary to implement risk-based measures such as policies and procedures, a screening process, terms and conditions in counterparty agreements, and regular training. These should meet applicable standards such as those in the recently issued "Framework for OFAC Compliance Commitments." A government-imposed compliance program is apt to be more complex and costly.

Though each case is different, using a checklist such as the above will help ensure best practices are followed.

Kirkland & Ellis lawyers **Mario Mancuso**, **Sanjay Mullick**, **Anthony Rapa** *and* **Abigail Cotterill** *are members of the firm's international trade and national security practice.*