THE REVIEW OF
SECURITIES & COMMODITIES REGULATION
AN ANALYSIS OF CURRENT LAWS AND REGULATIONS AFFECTING THE SECURITIES AND FUTURES INDUSTRIES

Vol. 51 No. 15 September 5, 2018

REDUCING THIRD-PARTY TRADE COMPLIANCE RISKS

The authors find that companies often overlook the risks posed by shortcomings in the trade compliance programs of their third-party business partners. In this article they describe two recent cases that illustrate such risks. They then suggest remedial steps in initial and follow-up due diligence, entering or renewing contracts, and responding to red flags.

By Peter Lichtenbaum and Eric Sandberg-Zakian *

The U.S. government maintains a far-reaching set of trade controls regulations, including economic sanctions targeting a variety of countries, regions, and persons; export controls on military, dual-use, and commercial goods, software, and information; and rules penalizing compliance with boycotts not approved by the U.S. government. Over the last decade, the U.S. government has enforced these laws aggressively, undertaking a growing number of inter-agency civil or criminal investigations, with some resulting in eye-catching penalties of hundreds of millions or even billions of dollars.

In recent years, corporate legal and compliance departments have become increasingly sensitive to the risk of trade controls violations and increasingly committed to implementing comprehensive compliance programs. In our experience, companies' efforts to comply with U.S. trade controls focus primarily on their own compliance measures. For example, a company will classify its products before exporting them from the United States or a company will screen its customer, the ultimate end-user, and any relevant financial institutions against government lists of restricted parties.

In contrast, companies often treat risk posed by shortcomings in the trade controls compliance programs of distributors and other third-party business partners as an afterthought. They are likely to focus on the risks of dealing with such partners from an anti-corruption compliance perspective, but they may overlook the trade compliance implications of those same relationships.

RECENT CASES

Two recent sanctions cases demonstrate the potential consequences of taking a hands-off approach to managing the risks posed by these relationships, and underscore the need to focus attention on the compliance activities of distributors and other third-party business partners.

* *PETER LICHTENBAUM co-chairs Covington & Burling LLP's International Trade and Finance Practice Group, and ERIC SANDBERG-ZAKIAN is an associate in the firm's White Collar Defense and Investigations Group. Their e-mail addresses are plichtenbaum@cov.com and esandbergzakian@cov.com.*

RSCR Publications LLC Published 22 times a year by RSCR Publications LLC. Executive and Editorial Offices, 2628 Broadway, Suite 29A, New York, NY 10025-5055. Subscription rates: $1,197 per year in U.S., Canada, and Mexico; $1,262 elsewhere (air mail delivered). A 15% discount is available for qualified academic libraries and full-time teachers. For subscription information and customer service call (937) 387-0473 or visit our website at www.rscrpubs.com. General Editor: Michael O. Finkelstein; tel. 212-876-1715; e-mail mofinkelstein@gmail.com. Associate Editor: Sarah Strauss Himmelfarb; tel. 301-294-6233; e-mail sarah.s.himmelfarb@gmail.com. To submit a manuscript for publication contact Ms. Himmelfarb. ISSN: 0884-2426.

The first recent case dealing with third-party business partner risk is *Epsilon Electronics, Inc. v. United States Department of the Treasury, Office of Foreign Assets Control*.[1] In 2014, the Treasury Department's Office of Foreign Assets Control ("OFAC") imposed a civil penalty of over $4 million on Epsilon, a California-based manufacturer of automotive electronic systems. OFAC imposed the penalty for 39 shipments of car audio and video equipment Epsilon sent to a distributor in Dubai called Asra. OFAC alleged that Epsilon knew or had reason to know that Asra would re-export the equipment to Iran, and that the shipments thus violated the Iran sanctions' prohibition on "the exportation, re-exportation, sale, or supply, directly or indirectly . . . of any goods, technology, or services to Iran" by U.S. persons, including exportation to a third country with "knowledge or reason to know" that the goods, technology, or services are "intended specifically" for re-exportation to Iran.[2]

Notably, however, OFAC did not have any evidence that the goods actually did arrive in Iran and, to the contrary, took the position that no such evidence was necessary to make out a violation. Instead, OFAC interpreted its regulation as prohibiting the exporter from sending goods to a third country with knowledge or reason to know the goods would be re-exported to Iran, regardless of whether they actually ended up there. Evidence that OFAC cited as giving Epsilon reason to know included information on Asra's website suggesting that, although the company's address was in Dubai, most or all of its sales were in Iran.

Epsilon challenged the penalty in federal district court in Washington, D.C. The district court upheld OFAC's penalty and the case was appealed to the D.C. Circuit. Although the D.C. Circuit ultimately ruled for Epsilon because OFAC did not offer a sufficient explanation for certain factual conclusions, the court affirmed OFAC's interpretation of its regulations. Specifically, the court agreed with OFAC that the applicable regulation prohibited Epsilon from shipping products to Asra in Dubai with reason to know that they would be re-exported to Iran, even if there was no way to know whether Asra actually did re-export them.

Thus, one key point to draw from the *Epsilon* case is that OFAC is inclined to impute to companies knowledge of sales activities described on their distributor's websites. While the lesson this point hammers home is perhaps a common one — do your due diligence on business partners carefully – the significant consequences in *Epsilon* are rather striking. Epsilon was penalized for making exports to Iran through Dubai based merely on the information available to Epsilon if it had undertaken basic due diligence, despite the fact that the government had no evidence that Asra ever actually re-exported the goods in question to Iran.

The second recent case dealing with third-party business partner risk is a December 2017 civil settlement between OFAC and the Delaware-based DENTSPLY SIRONA Inc.[3] DENTSPLY agreed to pay over $1.22 million to settle allegations that between 2009 and 2012, its non-U.S. subsidiaries exported 37 shipments of dental equipment and supplies from the United States to distributors in third countries, with knowledge or reason to know that the goods were ultimately destined for Iran. The level of knowledge that OFAC attributed to DENTSPLY's non-U.S. subsidiaries exceeded that attributed to Epsilon. In this case, OFAC alleged that the subsidiaries received confirmation that distributors were re-exporting DENTSPLY products to Iran and took steps to conceal that fact. OFAC also alleged that managers at the subsidiaries knew about and concealed the shipments at issue from DENTSPLY.

The fact that OFAC sought to penalize this conduct is unremarkable, given the degree of knowledge and active concealment by the subsidiaries' personnel. What is worth noting, however, is that DENTSPLY was penalized for dealings by its non-U.S. subsidiaries with non-U.S. distributors, even though DENTSPLY had no knowledge of those dealings and individual managers at the subsidiaries concealed the dealings from DENTSPLY. The lesson here is that it is not good

[1] 857 F.3d 913 (D.C. Cir. 2017).

[2] 31 C.F.R. § 560.204.

[3] OFAC, Enforcement Information for Dec. 6, 2017, https://www.treasury.gov/resource-center/sanctions/CivPen/Documents/20171206_Dentsply.pdf.

enough to do your own due diligence on business partners; you must ensure that your non-U.S. subsidiaries do theirs, as well.

The point underscored by *Epsilon* and *DENTSPLY* is that OFAC can hold companies responsible for their business partners' compliance lapses and that OFAC will expect proactive engagement with business partners to ensure transactions comply with U.S. trade controls. As *Epsilon* shows, OFAC will view generally available information about a distributor's business on the internet as raising red flags for all transactions, even in the absence of particular red flags with respect to individual transactions at issue. As *DENTSPLY* shows, OFAC will penalize a company if its non-U.S. subsidiaries have reason to know a transaction involves a sanctioned country, but conceal that knowledge from the parent company. Although both companies were formally penalized for knowing exports to Iran, the actual behavior that led to the penalty was failing to conduct sufficient due diligence on non-U.S. parties and failing to ensure those parties had adequate compliance programs.

Moreover, although both cases arise under OFAC's Iran sanctions, OFAC will no doubt apply this far-reaching approach to the concept of knowledge when dealing with business partners to other sanctions program. Likewise, the Department of Commerce has indicated it will take a similar approach to enforcing the Export Administration Regulations ("EAR").[4] In sum, companies are on notice that establishing their own compliance programs is not enough. They may also be held responsible for ensuring their business partners' programs are strong too.

STEPS FOR REDUCING RISK

Fortunately, there are a range of ways to mitigate third-party trade compliance risk. Opportunities to reduce risk can be found when conducting initial and follow-up due diligence, entering into or renewing contracts, and responding to red flags.

Communications with, and Due Diligence on, Business Partners

- *Review Publicly Available Materials.* During initial and follow-up due diligence, a company should make sure to review all available materials that would give the company reason to know of trade compliance issues. In *Epsilon*, OFAC looked to the distributor's website and publicly available information about the distributor's relationship with parties in Iran to prove Epsilon had reason to know that it was exporting products for sale in Iran. OFAC administers a compliance regime in which a company can be found to have exported goods to Iran on the basis of publicly available sources and in the absence of any evidence the specific goods at issue actually did go to Iran. Faced with that regime and other, similarly expansive trade controls regulatory regimes, companies must prioritize reviewing publicly available sources.

- *Ask Specific Questions about Restricted Parties and Destinations.* During initial due diligence and at periodic intervals thereafter, companies should ask their distributors or other key contractors whether they intend to export the company's products to any restricted persons or destinations, or have done so within the past five years. To ensure the question is clear to distributors, especially those outside the United States, companies should specify the destinations and denied-party lists at issue.

- *Review Business Partners' Compliance Materials.* If possible, companies should obtain and review copies of business partners' compliance materials. Taking steps to ensure that business partners have sufficient mechanisms in place to comply with U.S. trade controls will protect a company if those mechanisms ultimately fail and violations occur.

- *Educate Business Partners on Prospective Risks.* As a relationship between a company and business partner is beginning and compliance measures are under discussion, a company should consider

[4] The EAR provide that companies can be held to have reason to know of an impermissible end-use, end-user, or destination based on "red flags". EAR Part 732, Supplement No. 3.

Similarly, the Commerce Department's Bureau of Industry and Security ("BIS"), which administers the EAR, has stated that companies can be held liable for actions of third parties: "BIS recommends that you know your freight forwarder and customers. Not doing so puts your organization at risk. An untested or unproven freight forwarder can mishandle your item and your documentation, possibly putting your organization at risk of penalty. This is the case in routed transactions, when the foreign principal party in interest instructs the U.S. principal party in interest ("USPPI") to use a particular freight forwarder. The USPPI must document their due diligence to protect themselves from inaccurate Electronic Export Information entry, unauthorized shipping routes, and possible diversion." Export Compliance Guidelines, p. 12, *available at* https://www.bis.doc.gov/index.php/forms-documents/pdfs/1641-ecp/file.

offering training or information about U.S. trade controls to a business partner. Flagging key risks and tactics for preventing violations at the beginning of a business relationship can lead to improved compliance over the life of the relationship, as can making non-U.S. companies and unsophisticated U.S. companies aware that they may themselves face enforcement action for compliance failures.

Contracting

- *Strengthen Contract Provisions.* Companies entering into or renewing contracts with business partners should take the opportunity to optimize trade compliance provisions of the contracts. Important provisions include commitments to comply with U.S. trade controls (including specific commitments not to sell to sanctioned countries), requirements to screen counterparties against government lists of restricted parties, obligations to notify in the event of diversion or possible diversion, requirements to maintain a trade controls compliance program with certain elements, and audit rights to allow for reviewing sales data and compliance program implementation materials.

- *Ensure Key Provisions Are Flowed Down.* When a distributor or other business partner works with brokers or sub-distributors with which the company does not have a direct contract, the company should take steps to ensure that the business partners flow down core compliance requirements. Provisions that are most important to flow down include those relating to general compliance with U.S. and other applicable trade controls, and those specifically prohibiting dealings with restricted persons or destinations.

Responding to Red Flags

- *Document Discussions with Business Partners.* When red flags arise and companies engage with the relevant distributor or other business partner, they often resolve the matter by receiving additional details about the transaction at issue. All too often, these conversations happen by phone, not in writing, leaving a written record that does not reflect the prudent steps a company took to address a red flag. It is crucial to ensure that a written record of assurances provided by the business partner exists — ideally in an exchange of letters but alternatively in e-mail — and is preserved for the future.

- *Review Trends and Past Communications.* If a red flag regarding a particular transaction with a distributor or other business partner arises, the company should examine the transaction in depth, and look back at the original due diligence file and any readily available past communications that can reasonably be reviewed. Sometimes, patterns or trends turn out to be red flags, even if the individual communications or incidents comprising them were not obviously concerning when they occurred.

CONCLUSION

Of course, companies have different types of business partners and different relationships with their business partners. As a result, not all of these steps will make sense for all companies. But as *Epsilon* and *DENTSPLY* make clear, companies may well be held responsible for the trade compliance shortcomings of their distributors and other third-party business partners. Accordingly, companies should look for opportunities to prioritize addressing third-party business partner trade compliance risk. ■