Rushing to Buy PPE? Know the Red Flags for Profiteers

Matthew C. Luzadder, Constantine (Dino) Koutsoubas

May 26, 2020

The worldwide demand for personal protective equipment ("PPE") has drawn many new entrants to the market and opportunities for fraud and other illegal activity abound. In particular, there has been a rise in resellers, consultants and middlemen who offer to secure PPE in a competitive environment. Companies should not approach these transactions as ordinary retail sales contracts and should be aware of the particular risks that can arise in cross-border transactions that may involve foreign officials. Often, this risk mitigation involves conducting increased due diligence on potential business partners. Although these contracts may be entered into under pressure both due to market conditions and from counterparties eager to close a deal, lack of due diligence can lead to negative headlines.

In March, a Republican fundraiser and others started Blue Flame Medical LLC ("Blue Flame"), a PPE supply company that managed, roughly a week after its incorporation, to win a $12.5 million contract from the state of Maryland. According to the Washington Post, Blue Flame received a $6.25 million down payment in payment for providing the state with masks and ventilators within weeks.[1] After Maryland claimed that Blue Flame failed to deliver the PPE, it moved to cancel the contract and referred the matter to the state Attorney General.

In the same timeframe, Blue Flame was reported to have won a $600 million deal for masks in California, after receiving an "intriguing call" promising delivery of masks "that were sitting at the Port of Long Beach" and at below market prices.[2] After the state wired money to Blue Flame, however, its bank, using its normal vetting process, held up a $450 million down payment as a potentially fraudulent transaction. Blue Flame is now under investigation by California, Maryland, the Department of Justice, and Congress.[3]

In Chicago, Willie Wilson, a well-known local entrepreneur and former mayoral candidate, offered to procure masks for the city. Mayor Lori Lightfoot alleged that Wilson required the entire payment upfront—and in cash. Although there are a number of accounts of his conversations with government officials, Wilson explained that he needed the up-front payment to pay the manufacturers.[4]

The risks to the purchaser in these cases extend beyond fraud where a seller demands a substantial upfront payment to acquire and deliver PPE with greater speed and efficiency than established market players. Many of these offers involve leveraging the seller's relationships on a number of public and private levels. For example, third parties may appear in the transaction—often as purported consultants—claiming to have special connections to foreign officials or sources of PPE. This "red flag" most often appears in deals involving countries, such as China, where many of the suppliers of PPE are state-owned. It is also important to remember that employees of state-owned companies, including laboratories and hospitals in China, have been found to be foreign officials, and

bribes and other inducements authorized, offered, or paid to them to use their official discretion to obtain business have been found to violate the FCPA.

Purchasing companies must therefore be alert to the possibility that its substantial upfront payment is being used, in part, to bribe a foreign official in violation of anti-bribery requirements of the Foreign Corrupt Practices Act ("FCPA"). *See* 15 U.S.C. §§78dd-1, *et seq*. The FCPA's anti-bribery provisions prohibit payments to vendors made with the knowledge that (or willful blindness to the fact that) some of the money will be given to a foreign official for an improper purpose. 15 U.S.C. §§ 78dd-1(a)(3). The FCPA's prohibition applies not only to direct corrupt payments to a foreign official. It also applies to indirect payments made through third parties, such as consultants.

Any company conducting business abroad through third parties should therefore perform a risk-based evaluation of the parties based on the specifics of the proposed relationship. *See* U.S. DOJ Resource Guide to the FCPA (the "DOJ Guide").[5] If law enforcement discovers an improper payment, a purchasing company's liability may turn on an assessment of its willful blindness, assuming that the company did not know of the payment. In particular, law enforcement and regulators may ask what questions the company asked prior to engaging the third party and what the company did to resolve any red flags that arose during the due diligence process. Accordingly, a purchasing company should utilize a questionnaire based on the potential FCPA and fraud issues and maintain the responses received in its compliance files. Asking the U.S. Foreign Commercial Service to conduct basic diligence or a site visit to a vendor or intermediary's factory or office can also be a helpful, inexpensive diligence step.

In most cases, a purchasing company's due diligence should focus on any third-party consultants or facilitators of the transaction, as these parties have featured in many recent FCPA enforcement cases. Any third party's involvement in the transaction should have a legitimate rationale or business purpose and its compensation should reflect market realities, without being designed to disguise a hidden bribe to a foreign official. The third party's services should be well-defined by any agreement the purchasing company considers. Because a number of entities are entering the PPE space from other industries, perhaps out of altruism or because their core business has slowed, there are many new entrants who are legitimate actors. But there are others—including narco-traffickers who look to conceal contraband in PPE shipments—looking to take advantage of the pandemic for illegal purposes. [6]

Therefore, when evaluating a potential partner, it is particularly important that the company follow "know your partner" or "KYP" procedures. These including evaluating the business "track record" of any counterparty, its qualifications in performing these types of services, documentation supporting a conclusion that its fees are customary and reasonable, and appropriate banking and credit references. Of course, where basic due diligence questions are left unanswered or answered in an evasive way, those areas require enhanced due diligence, which in some cases, may entail going to a number of independent sources to confirm the potential business partner's claims.

Finally, although beyond the scope of this alert, a company needs to make sure that its products are safe and effective. The Centers for Disease Control and Prevention ("CDC") has noted that several counterfeit respirators have made their way into the U.S. market and has started posting examples on its website.[7] A purchasing company can use a number of methods as part of the KYP process to address risks associated with counterfeit goods. Federal customs agents are seizing import shipments of certain counterfeit and non-qualifying PPE, and getting these items released from seizure can be time consuming at best. Companies should work to ensure that the financial and regulatory risk of seizure is allocated to the supplier, not themselves as the importer, or to be sure

that the goods definitely qualify for the stated end use. Making assumptions in this area has been very costly to many companies.

Although the worldwide demand for PPE creates time pressure and a sense of urgency in securing a contract, companies must keep in mind that high pressure tactics to close a deal can also be a red flag, as many cross-border transactions require additional due diligence that may take more than a few days. At a minimum, the company should consider, before entering into any contract—and certainly before supplying any down payment—what due diligence policies and procedures will protect the company from unknowingly participating in a corrupt payment or other unlawful activity during the course of the transaction. Will the company be able to demonstrate that it knew and could justify the presence, role, and qualifications of each party in the transaction? If not, it should pause and conduct further diligence before proceeding.

To discuss your organization's compliance strategies in light of COVID-19, please contact a member of Kelley Drye & Warren LLP's White Collar Crime, Investigations and Compliance Practice Group.

---

[1] https://www.washingtonpost.com/politics/maryland-cancels-125-million-ppe-contract-with-firm-started-by-gop-operatives/2020/05/02/b54a14f0-8cbe-11ea-8ac1-bfb250876b7a_story.html

[2] https://calmatters.org/health/coronavirus/2020/05/blue-flame-deal-masks-investigation-wire-transfer-lawmakers-oversight-ma/

[3] https://www.wsj.com/articles/congress-to-investigate-protective-gear-supplier-blue-flame-11589299028

[4] https://www.chicagotribune.com/coronavirus/ct-coronavirus-chicago-lightfoot-wilson-20200420-gjrb3olrpvburpiecrmhgoahqi-story.html?outputType=amp

[5] *See generally* DOJ Guide, available at https://www.justice.gov/criminal/fraud/fcpa/guidance/guide.pdf

[6] https://www.khaleejtimes.com/coronavirus-pandemic/drug-traffickers-using-covid-19-ppe-consignments-to-hide-contraband

[7] https://www.cdc.gov/niosh/npptl/usernotices/counterfeitResp.html