akerman

Blog Post

Buyer Beware – FBI Warns of Fraud Involving Procurement of PPE and Other COVID-19 Supplies

April 21, 2020
By Elizabeth F. Hodge

Many employers are now making plans to have their employees return to the workplace. Based on recent alerts from the FBI, part of preparing to protect workers from COVID-19 at work should include protecting the company from falling prey to fraudsters. To do that, employers should put in place procedures to carefully screen vendors from whom they will purchase COVID-19 supplies needed to comply with CDC and OSHA guidance and protect their employees.

The FBI issued alerts on March 27, 2020, and April 13, 2020, in which it described rapidly emerging fraud schemes related to the procurement of personal protective equipment (PPE), medical equipment, and other goods and products in short supply due to the COVID-19 pandemic. While the alerts are directed to the medical community since to-date it has been the primary purchaser of COVID-19-related medical equipment and supplies, employers across all industries who are or will be seeking PPE should review the alerts and take appropriate steps to avoid being victimized by fraudsters.

The FBI warns of several types of schemes that fraudulent actors may engage in to take advantage of the dire need for PPE, medical equipment like

Related People

Elizabeth F. Hodge

Related Work

Healthcare
Labor and Employment

Related Offices

West Palm Beach

HR Defense Blog

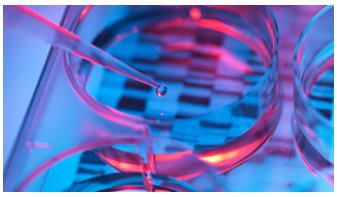
Akerman Perspectives on the Latest Developments in Labor and Employment Law

Visit this Akerman blog

Coronavirus Resource Center

Visit the Resource Center

ventilators, and other supplies and equipment in short supply during the pandemic:



- Scammers may promise supplies and equipment to which they do not have access.
- Fraudulent brokers and sellers may request that buyers wire funds before receiving the supplies or equipment and then deliver little or nothing in return.
- Bad actors may engage in business email compromise (BEC) schemes where they spoof a legitimate known email address or use a nearly identical email address to communicate with a victim to redirect legitimate payments to a bank account they control.

It is important to note that the FBI is not saying that legitimate manufacturers of PPE and other COVID-19 supplies are involved in these schemes; rather, the bad actors claim to be distributors or sellers of legitimate products.

Warning Signs

As employers start or continue to source PPE and related supplies for their employees, they should keep in mind the old saying, “if it sounds too good to be true, it probably is.” More specifically, employers should be alert to the following warning signs that the “seller” may not be legitimate:

- The seller contacts the buyer from a difficult to verify channel, e.g., telephone or email.
- The buyer does not currently do business with the purported seller, e.g., the would-be seller is not an already-approved vendor.
- The seller demands unusual payment terms, e.g., demands up-front payment or proof of payment.
- The seller cannot clearly explain how it happens to have a large supply of goods that are known to be in short supply.

- The potential purchaser cannot verify with the product manufacturer that the seller is a legitimate distributor of the product or otherwise verify that the supply chain is legitimate.
- The seller requires that funds be transferred immediately or makes a last minute change in previously established wiring instructions.
- The seller makes last-minute price changes or last-minutes excuses for a delay in shipment.

Employers should also be alert to counterfeit products and can find more information about unapproved or counterfeit PPE here.

How Employers Can Protect Themselves

While it is unfortunate that some unscrupulous actors will try to take advantage of the large demand for PPE and related supplies, businesses can protect themselves and their employees by implementing some simple steps to vet prospective vendors. To make sure that they are dealing with bona fide sellers or distributors, the FBI recommends that employers and other purchasers consider the following strategies:

- If the seller claims to be affiliated with an entity with an existing relationship with the employer, verify the vendor with a known contact; do not contact the vendor through an email or phone number it provides.
- If immediate delivery is not possible, route funds to a domestic escrow account from which the funds can be released when the goods are delivered.
- Verify with the manufacturer or a verified distributor that the seller is a legitimate distributor or vendor for the goods being offered.
- Where possible, have a trusted independent party verify that the goods for sale are as represented and presently available for sale.

- Question last minute changes in wiring instructions or recipient account information – do not re-route payment without independently verifying the source of the change instructions.
- Verify the email address the would-be seller uses to send emails, especially when using a mobile phone, by ensuring the sender's email address appears to match who it is coming from.

Also, because COVID-19 supply chain fraud schemes continue to evolve, businesses should periodically consult the FBI's coronavirus resources page.

Businesses that suspect they may have been the victim of COVID-19 fraud scheme may contact the FBI's Internet Crime Complaint Center.

If you need further assistance or guidance on COVID-19 and the workplace, contact your Akerman attorney.
