

April 13, 2020

<https://www.fbi.gov/news/pressrel/press-releases/fbi-warns-of-advance-fee-and-bec-schemes-related-to-procurement-of-ppe-and-other-supplies-during-covid-19-pandemic>

## **FBI Warns of Advance Fee and BEC Schemes Related to Procurement of PPE and Other Supplies During COVID-19 Pandemic**

The Federal Bureau of Investigation is providing this industry alert to warn government and health care industry buyers of rapidly emerging fraud trends related to procurement of personal protective equipment (PPE), medical equipment such as ventilators, and other supplies or equipment in short supply during the current COVID-19 pandemic.

The FBI recently became aware of multiple incidents in which state government agencies, attempting to procure such equipment, wire transferred funds to fraudulent brokers and sellers in advance of receiving the items. The brokers and sellers included both domestic and foreign entities. In one case, an individual claimed to represent an entity with which the purchasing agency had an existing business relationship. By the time the purchasing agencies became suspicious of the transactions, much of the funds had been transferred outside the reach of U.S. law enforcement and were unrecoverable.

The current environment, in which demand for PPE and certain medical equipment far outstrips supply, is ripe for fraudulent actors perpetrating advance fee and business email compromise (BEC) schemes, such as those described above.

In advance fee schemes related to procurement, a victim pre-pays (partially or in full) a purported seller or a broker for a good or service and then receives little or nothing in return.

BEC schemes often involve the spoofing of a legitimate known email address or use of a nearly identical email address to communicate with a victim to redirect legitimate payments to a bank account controlled by fraudsters. A variation on BEC schemes can involve similar social engineering techniques via phone call.

### **Risk Factors**

While pre-payment is more common in the current environment, it substantially increases the risk of a buyer being defrauded and eliminates most potential recourse. The following indicators are warning signs that an offer to sell items may not be legitimate:

- A seller or broker initiates the contact with the buyer, especially from a difficult to verify channel such as telephone or personal email.
- The seller or broker is not an entity with which the buyer has an existing business relationship, or the buyer's existing business relationships are a matter of public record.
- The seller or broker cannot clearly explain the origin of the items or how they are available given current demand.
- The potential buyer cannot verify with the product manufacturer that the seller is a legitimate distributor or vendor of the product, or otherwise verify the supply chain is legitimate.

- Unexplained urgency to transfer funds or a last minute change in previously-established wiring instructions.

## **Mitigation Recommendations**

The FBI recommends that buyers consider the following recommendations to protect their companies or agencies:

- If the seller claims to represent an entity with an existing relationship to the buyer, verify claims through a known contact—do not contact the vendor through information provided in an email or phone communication.
- If possible, have a trusted independent party verify the items for sale are physically present and of the promised make, model, and quality, and take delivery immediately upon payment.
- If immediate delivery is impossible, route payments to a domestic escrow account to be released to the seller upon receipt of the promised items.
- Verify with the manufacturer or verified distributor that the seller is a legitimate distributor or vendor for the items being offered.
- Be skeptical of last minute changes in wiring instructions or recipient account information—do not re-route payments without independently verifying the direction came from an authorized party.
- Verify the email address used to send emails, especially when using a mobile or handheld device, by ensuring the sender's email address appears to match who it is coming from.

If you think your company or agency is the victim of a fraud scheme related to COVID-19 immediately contact the FBI's Internet Crime Complaint Center at [ic3.gov](https://ic3.gov).

**For accurate and up-to-date information about COVID-19, visit:**

- [coronavirus.gov](https://coronavirus.gov)
- [cdc.gov/coronavirus](https://cdc.gov/coronavirus)
- [usa.gov/coronavirus](https://usa.gov/coronavirus)
- [fbi.gov/coronavirus](https://fbi.gov/coronavirus)
- [justice.gov/coronavirus](https://justice.gov/coronavirus)