Covid-19 Procurement Fraud

Protect your organization

By Victor Hartman, JD, CPA, CFF, CFE, and Debra L. McGlaun, CPA, CFE

Covid-19 is wreaking havoc on the supply chain of goods worldwide. The Federal Bureau of Investigation (FBI) reports that procurement frauds are on the rise. The healthcare sector is particularly vulnerable because of shortages of medical commodities, including personal protective equipment (PPE), ventilators, medical equipment, testing supplies and pharmaceuticals.

The United Nations and the World Health Organization (WHO) have established a Supply Chain Task Force to address the issue of rising demand, panic buying, hoarding and misuse. Early in the pandemic, the WHO reported that each month 89 million medical masks, 76 million examination gloves and 1.6 million goggles are required for the Covid-19 response.[1]

The surge in demand for medical commodities creates challenges for the procurement functions of healthcare organizations. They may be required to deviate from their best practices, take shortcuts and resort to utilizing a sole source or making emergency purchases from unknown vendors. The pressure to meet urgent patient care demands may result in organizations being defrauded.

In a federal prosecution, a Georgia man was charged with defrauding the Department of Veterans Affairs (VA). He is accused of making a series of fraudulent misrepresentations to secure orders from the VA for 125 million face masks and other PPE that would have totaled over $750 million.

He was also charged with promising that he could obtain millions of genuine 3M masks from domestic factories when he knew that fulfilling the orders would not be possible. He made similar false representations to other entities to enter into other fraudulent agreements to sell PPE to state governments.[2]

The FBI reports that procurement frauds are occurring primarily in two different ways: advance fee scheme and business email compromise.[3]

Advance fee scheme

Fraudsters purport to sell supplies and equipment to which they do not have access, in what is known by law enforcement as an advance fee scheme. A fraudulent broker requests wired funds before the purchaser receives product and then delivers nothing in return. The Federal Trade Commission reports one of the most common

[1] www.who.int/news-room/detail/03-03-2020-shortage-of-personal-protective-equipment-endangering-health-workers-worldwide
[2] www.justice.gov/opa/pr/georgia-man-arrested-attempting-defraud-department-veterans-affairs-multimillion-dollar-covid
[3] 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

A purchaser must conduct substantial due diligence when dealing with a vendor purporting to sell Covid-19-related goods.

Covid-19 frauds is the online purchase of goods that never arrive.

Red flags – A purchasing agent should evaluate several risk factors before executing a purchase. Because prepayment for goods is more common in the current environment, the risk of a purchaser being defrauded is substantially increased and eliminates the usual recourse options. The FBI offers the following indicators as 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 channel that's difficult to verify such as telephone, or through personal email.
- The seller or broker is not an entity that the buyer has an existing business relationship with, or the buyer's existing business relationships are a matter of public record, enabling a fraudster to pose as a legitimate vendor.
- 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.
- An unexplained urgency to transfer funds or a last-minute change in previously established wiring instructions occurs.

Mitigation recommendations – Your procurement and financial management should consider the following FBI recommendations to protect your organization from an advance fee scheme:

- Verify with the manufacturer or a verified distributor that the seller is a legitimate distributor or vendor for the items being offered. If the seller is claiming to have an existing relationship, verify through another known contact. Do not contact the vendor through information provided by email or phone.
- 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.
- 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.

The bottom line is that the purchaser must conduct substantial due diligence when dealing with a vendor purporting to sell goods, particularly those related to Covid-19.

Business email compromise (BEC)

The FBI reports that fraudsters are exploiting the BEC fraud that has been repurposed for Covid-19. The scam involves convincing an organization insider to wire transfer funds to the fraudster.

The BEC fraud was the most devastating fraud worldwide in terms of both prevalence and dollar loss before Covid-19. Fraudsters are now using Covid-19 to target healthcare organizations' procurement functions. The essence of the BEC is to convince a procurement or financial official to wire transfer funds to the fraudster. The victim may be targeted through spear phishing, social engineering, email spoofing, or the use of malware.

Although the techniques vary, the fraudsters want to find a way to communicate with a financial insider via email. The latest twist in the scheme is to advise the victim that the bank commonly used to accept receipt of funds has now changed. The FBI reports that fraudsters' explanations include that the bank account changed "due to the Coronavirus outbreak and quarantine processes and precautions" and the regular bank accounts were inaccessible due to "Corona Virus audits."[4]

The BEC scheme often involves spoofing a legitimate email address or using a nearly identical email address to communicate with a victim to redirect legitimate payments to a bank account controlled by the fraudsters. For example, the email address jaysmithh@hospital.com has an extra h after Smith. Without training and awareness, many employees will simply miss this telltale sign of fraud. A variation on BEC schemes can involve similar social engineering techniques via a phone call.

[4] www.fbi.gov/news/pressrel/press-releases/fbi-anticipates-rise-in-business-email-compromise-schemes-related-to-the-covid-19-pandemic

Red flags – The FBI lists red flags for the BEC fraud[5]:

- An unexplained urgency by the seller
- A last-minute change in the wire instructions or recipient account information
- A last-minute change in the established communication platforms or email account address
- Communications occur only through email and the seller refuses to communicate via telephone or online voice or video platforms
- A seller requests an advance payment of services when not previously required
- The seller requests the purchaser to change the direct deposit information

Mitigation recommendations – Your procurement and financial management staff should consider the following recommendations to protect your organization from the BEC scheme:

- Verify any changes to the vendor's contact information or bank routing information on file—do not contact the vendor through the number provided in the email.
- Be alert to hyperlinks that may contain misspellings of the actual domain name.
- Verify that the purported email address used to send the email matches the actual address it was sent from. To do this, compare the Send address you see on the email to the Send address in the header information.[6]

Other frauds

Unfortunately, the healthcare industry is also experiencing numerous other frauds related to Covid-19. Emerging fraud schemes include the bogus sale of vaccines, Covid-19 tests and antibody tests. Fraudsters are also gaining access to personally identifiable information (PII) through the promotion of Covid-19 healthcare products and services.

The fraudsters use the PII to commit traditional identity theft frauds including a popular scheme to fraudulently apply online for unemployment insurance benefits.

The Coronavirus Aid, Relief, and Economic Security (CARES) Act is the largest stimulus program in U.S. history. Federal prosecutors are rapidly indicting businesses that have defrauded both the Paycheck Protection Program and the loan program by obtaining money under false pretenses. The magnitude of CARES Act fraud will not be known for years. The defrauding of these federal programs presents excellent opportunities for whistleblowers to obtain substantial rewards under the federal False Claims Act.

Other Covid-19 frauds are being used to attack unsuspecting victims. Fraudsters are promoting fake charities that purport to aid Covid-19 victims in the U.S. and worldwide. Phishing schemes are being used to compromise electronic devices or introduce ransomware.

In the pandemic environment, individuals naturally have a strong interest in educating themselves about Covid-19 issues. Fraudsters posing as authorities from the WHO or the Centers for Disease Control and Prevention are sending emails purporting to contain links to valuable information. One wrong click could compromise a victim's computer.

Conclusion

You and your organization must remain vigilant during the Covid-19 pandemic. The pandemic is causing staff charged with fighting fraud to work remotely. You and your colleagues must inform your internal staff about these unique frauds to have an effective fraud prevention program.

Among the many Covid-19 related frauds, the advance fee scheme is the most prevalent. The best way to prevent this scheme is to have a fraud awareness and prevention program and adequate vendor due diligence controls implemented by your procurement and financial departments. **NP**

Victor Hartman, JD, CPA, CFF, CFE, is Principal of The Hartman Firm, LLC, specializing in forensic accounting and internal investigations. He was an FBI Special Agent. He is now an Adjunct Professor at Georgia State University and serves on Georgia Southern University's Forensic Accounting Advisory Board. Vic can be reached at (404) 369-0616 and Vic@HartmanFirm.com.

Debra L. McGlaun, CPA, CFE, specializes in the development of internal control policies and procedures to help companies manage strategic, operational and regulatory compliance risks. She serves on the Georgia Society of Certified Public Accountants' Fraud and Forensic Council, Leadership Council, and Accounting and Auditing Conference Task Force. Debbie can be reached at DebbieMcGlaunCPA@gmail.com.

[5] Ibid
[6] https://frsecure.com/blog/is-that-sender-for-real-three-ways-to-verify-the-identity-of-an-email/