



OFFICE of PRIVATE SECTOR

LIAISON INFORMATION REPORT (LIR)



HEALTHCARE & PUBLIC HEALTH SECTOR

12 August 2020

LIR 200812006

PPE Fraud Scheme Targeting Healthcare Sector and Utilizing a False FBI Asset Verification Line to Steal PII

References in this LIR to any specific commercial product, process or service or the use of any corporate name herein is for informational purposes only and does not constitute an endorsement, recommendation, or disparagement of that product, process, service or corporation on behalf of the FBI.

The FBI's Baltimore Field Office, in coordination with Office of Private Sector (OPS), prepared this LIR to inform private sector partners about recent Personal Protective Equipment (PPE) fraud schemes targeting the Healthcare Sector. These schemes involved individuals receiving an email from a broker, who claimed to have access to a vendor with an unlimited supply of nitrile gloves and required potential buyers to contact and provide personal identifying information (PII) to an "FBI Verification Line" as part of the purchasing procedures. With the influx of various vendors selling PPE, it has become more difficult to distinguish fraudulent PPE distributors from legitimate ones. However, FBI asset verification lines do not exist, and the FBI has no role in brokering PPE deals or validating PPE suppliers. During these unprecedented times when organizations are looking to protect their workforce, and medical facilities are seeking to replenish their supplies, opportunists are continuously seeking to capitalizing on crucial necessities. In addition to great financial loss, the health and safety of essential front-line workers are at risk due to the purchase of counterfeit products or by PPE not being delivered as promised. These schemes create significant financial and physical safety vulnerabilities for medical professionals, medical facilities, the general public, and pandemic victims. This report can be read in conjunction with the following LIRs:

- **LIR 200323006**, "Criminals Exploiting COVID-19 Outbreak for Financial Gain through Procurement and Consumer Fraud," 23 March 2020
- **LIR 200410004**, "Criminals Exploiting COVID-19 Pandemic for Financial Gain through Procurement Fraud of Medical Equipment and Personal Protective Equipment (PPE)," 10 April 2020
- **LIR 200421003**, "Indicators of Fraudulent 3M Personal Protective Equipment," 21 April 2020
- **LIR 200422004**, "Individual(s) Targeting Hospital Staff to Solicit the Sale of COVID-19 Personal Protective Equipment (PPE) with a Fake Certification Letter in an Email," 22 April 2020
- **LIR 200601006**, "COVID-19 Shipping Fraud Scheme Targeting U.S. Businesses and Consumers," 01 June 2020

In June 2020, an identified vendor claimed to be in possession of between 10 and 20 billion boxes of 100 count nitrile gloves. According to a cooperating witness, individuals targeted by this fraud scheme received specific instructions to purchase the gloves:

1. All parties were first required to sign a Non-Circumvention, Non-Disclosure & Working Agreement
2. The buyer would then go online to submit a letter of intent
3. The vendor would generate a purchase order and asset purchase agreement to be signed by the buyer



OFFICE of PRIVATE SECTOR

LIAISON INFORMATION REPORT (LIR)



4. After signing an "Authorization to Verify" form, the buyer would receive a phone number for the "FBI Verification Line," which they would contact and be required to provide PII in order to verify their assets for the purchase
5. Once the vendor's and buyer's assets were verified, the buyer would be required to wire a 10 percent deposit to schedule a live inspection of the inventory
6. Following the inspection, the buyer would be required to immediately pay the remaining balance before receiving their purchase

The FBI has identified the following indicators that may help private sector partners recognize when they are being targeted by a PPE fraud scheme. These suspicious activities/indicators include but are not limited to any individual, group, or activity (*these indicators should be observed in context and not individually*):

- Unsolicited advertisements for PPE being sent to an organization or directly to personnel
- Vendors claiming to possess or have access to an unusually large inventory of gloves and other PPE (sometimes in the billions), especially considering ongoing supply chain shortages
- Vendors requiring refundable deposits or full payment prior to product inspection or delivery
- Vendors claiming FBI involvement in the asset/product verification process or providing a phone number in their buying procedures to contact an FBI asset verification line
- Vendors threatening criminal charges or law enforcement action if anyone other than the buyer contacts the FBI asset verification line

The FBI recommends the following proactive measures, which when paired with timely reporting to law enforcement, can help private sector organizations avoid becoming victims of PPE fraud schemes and mitigate potential financial loss or harm to personnel:





- Avoid online sales of PPE referencing an FBI asset verification line
- When ordering PPE from online retailers, always verify the Uniform Resource Locator (URL) and confirm "https" in the web address, as a lack of a security certification ("https") may be an indicator that the site is insecure or compromised
- If procuring other categories of PPE such as gowns, gloves, goggles, and face shields, directly consult the manufacturer to verify authenticity and availability
- Be wary of unprompted solicitations to purchase large quantities of PPE and do not respond by providing usernames, passwords, PII, or financial information

Should a vendor of PPE or other critical resources claim FBI involvement in any form, or if you believe your organization was the victim of PPE-related fraudulent activity, please contact your local FBI Field Office and report details regarding this incident to the Internet Crimes Complaints Center at <https://www.ic3.gov/default.aspx>.

This LIR was disseminated from OPS's Information Sharing and Analysis Unit. Direct any requests and questions to your FBI Private Sector Coordinator at your [local FBI Field Office](https://www.fbi.gov/contact-us/field-offices): <https://www.fbi.gov/contact-us/field-offices>.



Traffic Light Protocol (TLP) Definitions

Color	When should it be used?	How may it be shared?
<p>TLP:RED</p>  <p>Not for disclosure, restricted to participants only.</p>	<p>Sources may use TLP:RED when information cannot be effectively acted upon by additional parties, and could lead to impacts on a party's privacy, reputation, or operations if misused.</p>	<p>Recipients may not share TLP:RED information with any parties outside of the specific exchange, meeting, or conversation in which it was originally disclosed. In the context of a meeting, for example, TLP:RED information is limited to those present at the meeting. In most circumstances, TLP:RED should be exchanged verbally or in person.</p>
<p>TLP:AMBER</p>  <p>Limited disclosure, restricted to participants' organizations.</p>	<p>Sources may use TLP:AMBER when information requires support to be effectively acted upon, yet carries risks to privacy, reputation, or operations if shared outside of the organizations involved.</p>	<p>Recipients may only share TLP:AMBER information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm. Sources are at liberty to specify additional intended limits of the sharing: these must be adhered to.</p>
<p>TLP:GREEN</p>  <p>Limited disclosure, restricted to the community.</p>	<p>Sources may use TLP:GREEN when information is useful for the awareness of all participating organizations as well as with peers within the broader community or sector.</p>	<p>Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels. Information in this category can be circulated widely within a particular community. TLP:GREEN information may not be released outside of the community.</p>
<p>TLP:WHITE</p>  <p>Disclosure is not limited.</p>	<p>Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release.</p>	<p>Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.</p>