



# OFFICE of PRIVATE SECTOR

LIAISON INFORMATION REPORT (LIR)



## CROSS-SECTOR

23 March 2020

LIR 200323006

### Criminals Exploiting COVID-19 Outbreak for Financial Gain through Procurement and Consumer Fraud

The FBI Criminal Investigative Division (CID), in coordination with the Office of Private Sector (OPS), prepared this LIR to address criminal exploitation of the global supply chain disruptions and manufacturing shortages resulting from the novel coronavirus (COVID-19) outbreak. Recent reporting from multiple sources indicates an increase in financial fraud schemes, as scammers have seized upon the ever-growing demand for Personal Protective Equipment (PPE)<sup>a</sup> to target healthcare providers and the general public. Many of the schemes attempt to capitalize on high demand, low supply PPE such as N95 National Institute for Occupational Safety and Health (NIOSH)-approved respirator masks, which are among the required PPE for healthcare personnel responding to COVID-19.

The FBI has identified the following proactive measures for consumers and procurement personnel to help mitigate financial loss or the purchase of potentially harmful counterfeit N95 masks. These recommendations are not meant to be an exhaustive list of guidance regarding COVID-19:

- 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
- Consult the U.S. Centers for Disease Control and Prevention (CDC) NIOSH website to view a list of all NIOSH approved manufacturers of N95 respirator masks and validate approval and certification numbers<sup>b</sup>
- Confirm N95 respirator mask approval status and certification numbers using the NIOSH flyer (Figure 1), the NIOSH website, or the CDC website, which includes examples of identified counterfeit or unapproved N95 respirator masks<sup>c</sup>
- If procuring other categories of PPE such as gowns, gloves, goggles, and face shields, consult the manufacturer to verify authenticity and availability
- Be wary of unprompted solicitations to purchase large quantities of PPE and do not provide usernames, passwords, personal identifying information (PII) such as social security number and date of birth, or financial information in response to an email or robocall

<sup>a</sup> Personal Protective Equipment is defined by the Occupational Safety and Health Administration (OSHA) as, “specialized clothing or equipment, worn by an employee for protection against infectious materials.” The CDC has identified gowns, gloves, goggles or full-face shields, and N95 respirator masks as required PPE for COVID-19.

<sup>b</sup> [https://www.cdc.gov/niosh/npptl/topics/respirators/disp\\_part/default.html](https://www.cdc.gov/niosh/npptl/topics/respirators/disp_part/default.html)

<sup>c</sup> <https://www.cdc.gov/niosh/npptl/usernotices/counterfeitResp.html>



# OFFICE of PRIVATE SECTOR

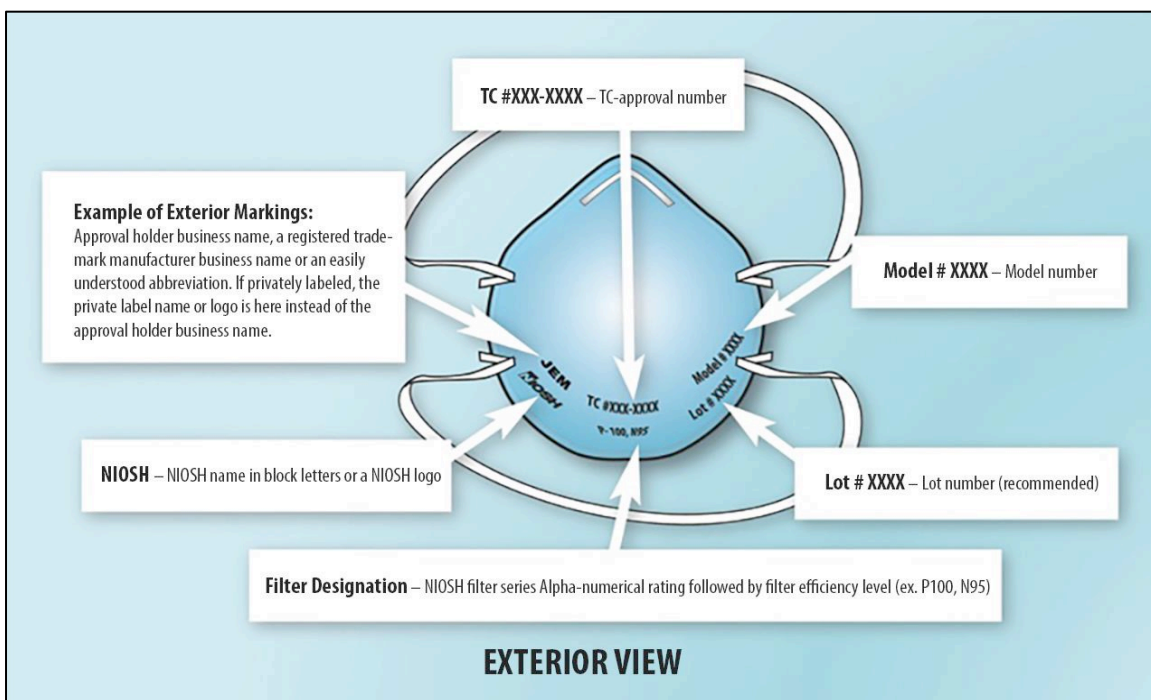
LIAISON INFORMATION REPORT (LIR)

As of 11 March 2020, many large U.S. retailers and suppliers have sold out of their N95 respirator mask inventories and are now warning consumers against the rise of counterfeit versions. A survey of safety masks and respirators on one U.S. e-commerce platform found at least one hundred product listings that were counterfeit or unapproved. Between 1 December 2019 and 11 March 2020, procurement entities and distributors looking to source N95 respirator masks and protective gowns reported combined losses exceeding \$3.6 million. The most common scam was the solicitation and subsequent non-delivery of purchase orders of N95 respirator masks and protective gowns after victims sent money. In at least one FBI complaint in February 2020, an alleged fraudster conducted a non-delivery scam and contacted the victim to say their product was delayed due to trade disruptions resultant of COVID-19.

If you believe your organization has purchased counterfeit PPE or COVID-19 testing kits, or were the victim of a fraud or scam, please contact your local FBI Field Office and report details regarding this incident to the Internet Crimes Complaints Center at [IC3.gov](https://www.ic3.gov) and/or the National Intellectual Property Rights Coordination Center at [IPRCenter.gov](https://www.iprcenter.gov). Due to global shortages and prioritization of healthcare institutions, the CDC advises only healthcare personnel, infected individuals, and those caring for infected individuals obtain N95 respirator masks. The best source for accurate, up-to-date information is the U.S. CDC at <https://www.cdc.gov/> and <https://www.coronavirus.gov/>.

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 [www.fbi.gov/contact-us/field-offices](https://www.fbi.gov/contact-us/field-offices).





**Figure 1: Generic sample of a respirator mask with appropriate markings**



Source: NIOSH website at [https://cdc.gov/niosh/npptl/topics/respirators/disp\\_part/default.html](https://cdc.gov/niosh/npptl/topics/respirators/disp_part/default.html)



**Traffic Light Protocol (TLP) Definitions**

Color	When should it be used?	How may it be shared?
<p><b>TLP:RED</b></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><b>TLP:AMBER</b></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. <b>Sources are at liberty to specify additional intended limits of the sharing: these must be adhered to.</b></p>
<p><b>TLP:GREEN</b></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><b>TLP:WHITE</b></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>