RECRUITING SCAM ADVISORY

Please be advised that unauthorized individuals may attempt to use the Olin Corporation ("Olin") name or brand, or the name of Olin directors and employees, in an attempt to secure personal or financial information, or money, from job seekers. These scammers use a variety of tactics, including posting false job postings on job boards, LinkedIn® and other locations, and sending unsolicited emails, text messages or other communications to job seekers, falsely representing themselves to be affiliated with Olin.

The following are some important signs to look for in determining whether you may be the target of a scam:

- Check the email address origin. Olin employees should have an email address ending in @olin.com or @olinbc.com. Scammers will try to make very similar email address domains, so make sure to check that it is from a @olin.com or @olinbc.com address.
- A communication requests money for placement fees, recruiting, or in exchange for guaranteed employment. Any communication requesting any amount of money in exchange for employment with Olin is fraudulent. Olin never charges candidates fees, or requires payments of any kind in order to secure employment.
- A communication requests payment as a fee for certification, training materials, office equipment or other work-related expenses. Olin does not require payment for any materials or equipment as part of its recruiting process.
- **Requests for tax, bank account or credit card information.** Olin recruiters do not require the completion of tax forms, or request bank account or credit card information as part of the recruiting process. As a precaution, we recommend you do not disclose personal or financial details to anyone in response to an unsolicited email request.

You may also have been contacted directly by a scammer who may have obtained your resume through a resume database. As a federal contractor, Olin is committed to equal opportunity employment and all valid, open positions will be posted on our website (<u>www.olin.com</u>) and all interested applicants must apply on-line. We do not accept paper applications except in limited circumstances and we do not directly solicit individuals for any role that is not posted on our website. We do not conduct interviews via text or an instant messaging application (like Google Hangout).

If you are contacted regarding a fraudulent employment proposal or have been the victim of a recruiting scam, you are encouraged to alert your local law enforcement agency.

The <u>Federal Trade Commission also has a reporting service on their website</u> for those who have been targeted by a recruiting scam.