ALERT: BEWARE OF FRAUDULENT ONLINE EMPLOYMENT SCAMS

Please be advised that we have recently become aware of online scams involving fraudulent parties extending job offers claiming to be from The CooperCompanies, CooperVision, or CooperSurgical. These fraud schemes are designed to obtain confidential personal information from their targets, such as driver's license, social security, birth certificate, and banking information. These fraud schemes are very sophisticated and often impersonate actual company employees. The impersonators set up fake interviews using online chat platforms and may send fake checks to applicants.

CooperCompanies, CooperVision, and CooperSurgical do <u>not</u> conduct candidate interviews via any social media chat forum or app. If you have questions about verifying whether a career opportunity or communication is legitimate, please contact us at one of the numbers listed below. Additionally, If you suspect you are the target of a scammer who is unlawfully misrepresenting themselves as our company representatives, we encourage you to contact us.

CooperCompanies – (925) 460-3600 CooperVision- (585) 756-9500 CooperSurgical- (203) 601 -5200

More information on fraudulent employment scams is available from the FBI: <u>Internet Crime</u> <u>Complaint Center (IC3) | Cyber Criminals Use Fake Job Listings To Target Applicants' Personally Identifiable Information</u>

- If you believe you are a victim, please contact law enforcement and/or the FBI Internet Crime Complaint Center IC3: https://www.ic3.gov/
- If you believe you have received a fraudulent check, please consult with the Federal Trade Commission: https://www.consumer.ftc.gov/articles/how-spot-avoid-and-report-fake-check-scams and if you have deposited a fraudulent check, notify your bank immediately.
- If you believe you may have been a victim of identity theft as a result of information provided to
 a scammer, please review available resources here: https://www.identitytheft.gov/, notify law
 enforcement, and take all possible steps to avoid becoming the victim of criminal activity on the
 internet.