Statement Regarding Job Offer Fraud Scams

Beware of Fraudulent Recruiting Advertisements and Scams

Be aware when applying for a job, there are job offer scams perpetrated through the use of the Internet and social media platforms scamming people with fake job offers to gather personal and financial information. The scams prey upon those seeking employment and use false and fraudulent offers of employment with companies such as EyePoint to steal from their victims. EyePoint believes that one of the best ways to put a stop to these types of scams is to make you aware that they exist, provide tips on how to identify and avoid them, and make clear how we recruit for positions with EyePoint so that you can more easily identify fraudulent recruiting advertisements.

- No applicant for employment with EyePoint is ever required to pay any money as part of the job application or hiring process.
- EyePoint never interviews job applicants through chat rooms (such as Google Hangouts), or through instant messaging systems. If someone tells you that they want to interview you for a job through a chat room, via text or instant messaging, they do not work for or represent EyePoint and are likely seeking to defraud you.
- EyePoint's job recruitment process involves in person and/or telephonic interviews and occasionally via Skype.
- EyePoint's job recruiting staff sends email communications to job applicants from "@eyepointpharma.com" email accounts only. Any email that states to be from EyePoint but does not have a "@eyepointpharma.com" address should be assumed to be fraudulent.

Recognizing a Potential Recruiting Fraud

Despite the fact that EyePoint cannot predict all the ways scammers might operate in the future, the following is a non-exclusive list of warning signs of recruiting fraud:

- You are asked to provide credit card, bank account number(s) or other personal financial information as part of the "job application" process.
- The contact email address contains a domain other than "@eyepointpharma.com," such as "@live.com," "@gmail.com," "@yahoo.com," "@outlook.com," or another personal email account.
- The position requires an initial monetary investment, such as a payment by wire transfer.
- The posting includes spelling errors, grammatical errors, syntax errors, or otherwise appears to have been written by someone not fluent in English.
- You are offered a payment or "reward" in exchange for allowing the use of your bank account (e.g., for depositing checks or transferring money related to promised employment).
- You are asked to provide a photograph of yourself.
- The job posting does not mention required qualifications and job responsibilities, but instead focuses on the amount of money supposedly to be made.
- The job posting reflects initial pay that is high compared to the average compensation for the type of job.
- The supposed "employer" contacts you by phone or through a chat room or instant messaging service, and gives no way to call them back or the number they do give is not active or goes only to a voicemail box. For example, such supposed "employers" often direct that you "meet" them in chat rooms at specific times.

What You Can Do

- If you believe you have been the victim of a job recruiting fraud scam, you can:
- File an incident report at http://www.cybercrime.gov,
- Call the Federal Trade Commission at **1-877-FTC-HELP** (1-877-382-4357).
- File a complaint with the Federal Bureau of Investigation at https://ic3.gov
- Contact your local police to report the fraud.
- Contact your bank or credit card company to close your account and dispute any charges related to the fraud.