BAUSCH + LOMB
See better. Live better.

Statement Regarding Job Recruiting Fraud Scams

Beware of Fraudulent Recruiting Advertisements

If you are applying for a job at Bausch + Lomb you should be aware that there are people trying to trick and scam you with fake job offers to gather personal and financial information. These scammers will try to use information they get from you to steal your money using the Internet and social media. These scammers frequently misappropriate and use a company's logo, names and photographs of its executives, and detailed information about the company, to make it look like they are legitimate representatives of a company. The scams prey upon those seeking employment, and use false and fraudulent offers of employment with companies such as Bausch + Lomb to steal from their victims. Bausch + Lomb 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 Bausch + Lomb so that you can more easily identify fraudulent recruiting advertisements:

- Bausch + Lomb never requires any job applicants to pay money to anyone (Bausch + Lomb or anyone else) as part of the job application or hiring process. If someone asks for money or offers to send you a check for training, equipment, etc. as part of a recruiting process, they do not work for or represent Bausch + Lomb and are likely seeking to defraud you.
- Bausch + Lomb only conducts job interviews in person, by telephone, and occasionally via Skype, and 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
- Bausch + Lomb and are likely seeking to defraud you.
- Bausch + Lomb's job recruiting staff only sends email communications to job applicants from a "@bausch.com" email address and do not use email accounts such as Yahoo and Gmail for recruiting purposes. You should assume that any email claiming to be from Bausch + Lomb that does not have a "@bausch" address is fraudulent and is not from Bausch + Lomb.

How to Recognize Potential Recruiting Fraud

The individuals who perpetrate frauds like this are continuously changing and evolving their methods, and one of the most important defenses is healthy skepticism based on the discussion above. Despite the fact that Bausch + Lomb 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 "@bausch.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