

Recruitment Fraud Statement

Beware of Recruiting Fraud

Job Applicants should be aware of job recruitment, interview, and offer scams being perpetrated through the use of the Internet and social media platforms. The scammers frequently misappropriate and use a company's logo and/or photos of its executives to give the appearance of legitimacy. The scam preys upon those seeking employment and uses false and fraudulent offers of interviews and/or employment with employers such as Ironwood to steal from the victims. Ironwood believes that one of the best ways to put a stop to this scam is to make you aware of it.

No applicant for employment with Ironwood is ever required to pay any money as part of the job application or hiring process, and Ironwood's job recruitment process involves in-person and/or telephonic interviews in most cases.

In addition, Ironwood's job recruiting staff sends email communications to job applicants from "@ironwoodpharma.com" email accounts only. Any email that purports to be from Ironwood but does not have a "@ironwoodpharma.com" address should be assumed to be fraudulent.

Recognizing Recruiting Fraud

The following are warning signs of recruiting fraud:

- You are required to provide your credit card, bank account number(s) or other personal financial information as part of the "job application" process.
- The open position does not appear on the company's website listing of job positions.
- The contact email address contains a domain other than "@ironwoodpharma.com", such as "@live.com", "@gmail.com", or another personal email account.
- The position requires an initial monetary investment, such as a payment by wire transfer.
- The posting includes spelling and grammatical errors.
- 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 employment).
- You are asked to provide a photo of yourself.
- The job posting does not mention required qualifications and job responsibilities, but instead focuses on the amount of money to be made.
- The job posting reflects initial pay that is high compared to the average compensation for the position type.

• The "employer" contacts you by phone, but there is no way to call them back or the number is not active or goes only to a voice message box.

What You Can Do

If you believe you have been the victim of job recruiting fraud, you can:

- File an incident report at: http://www.cybercrime.gov,
- Call the FTC at: 1-877-FTC-HELP (1-877-382-4357).
- File a complaint with the FBI at: https://ic3.gov
- Contact the local police to report the fraud.
- Contact your bank or credit card company to close the account and dispute the charges.