Note on Fraudulent Job Offers

Editas has received reports of people receiving fraudulent offers of employment from us. The fraudulent offer process includes individuals posing as Editas executives by email and text, conducting Skype interviews using the chat feature, and extending verbal and written fraudulent offers of employment. The persons making these fraudulent offers often request sensitive personal information as part of the "hiring process", including copies of drivers' licenses and IRS Form W-4 information.

How do I know if I received a fraudulent offer?

Fake interview requests, often sent by email or text, and offer letters, may include our logo or executive signature making them appear authentic. These emails and/or offer letters often look trustworthy at first blush, so vigilance is necessary. The only legitimate business email domain we use is @editasmed.com and our employees will never use a gmail or other personal email address to contact you. In addition, we will not contact you via text message or conduct an interview through chat.

If you applied for an Editas position on any website other than our Careers page, you may have been a target of the scammers and not involved in an actual Editas hiring process. You should promptly contact the Editas Human Resources Department at HumanResources@editasmed.com to verify the legitimacy of the job opportunity.

What should I do if believe I am the victim of a fraudulent employment scheme?

Legitimate Editas employees will never ask you to provide personal information or ID via email, text or telephone as part of our hiring process, and so under no circumstances should you provide any personal information to any recruiters, or make any purchases at their request. You should cease all further communication with these individuals, and under no circumstances should you click any links that they may have sent you.

If you received what you believe is a fake offer letter and provided any personal information or made purchases as part of a fraudulent offer process, we recommend you immediately:

- contact law enforcement to notify them that you may have been the victim of identity theft;
- contact your bank or credit card provider and let them know your account may have been compromised;
- contact your email provider — such as Gmail, Yahoo, or AOL — to alert them about the email address that was used in the fraudulent scheme.; and/or
- forward the message to HumanResources@editasmed.com.

To assist law enforcement in investigating these matters, please retain a copy of all correspondence relating to the fraudulent offer.

If you have been a victim of this scam, we sincerely regret the discomfort, inconvenience, and grief this incident may have caused you, as well as the time it has wasted in your job search. We sincerely appreciate your interest in Editas, and we encourage you to view our legitimate job postings on our Careers page.

Editas is not responsible for fraudulent offers or requests for personal information, and advises candidates to follow the guidance provided above.