RECRUITMENT FRAUD NOTICE

PROTECT YOUR PRIVACY

Baxter has discovered incidents of employment scams, where fraudulent parties pose as Baxter employees, recruiters, or other agents, and engage with online job seekers in an attempt to steal personal and/or, financial information. These unauthorized parties may use Baxter's name and logo to post jobs, engage with job seekers via instant message, LinkedIn, or chat rooms, or even extend offers via text message.

At Baxter, we do not ask for personal financial information during telephone, in-person or video interviews, nor do we make offers of employment without undergoing a thorough recruiting process. We also will not request a fee to be considered for a job.

Please read this notice in its entirety to learn how you can protect yourself against being a victim of recruitment fraud.

How will I know if I have been engaged as part of an online job-hunting scam?

There are several warning signs that might suggest you are being engaged as part of an online job-hunting scam. They may include:

- You receive an email from an individual claiming to be a Baxter recruiter, but the sender does not have an authorized baxter.com email address.
- Email messages use generic salutations such as sir/madam, rather than your name, or contain multiple typos and grammatical errors.
- The sender asks you to share personal information (home address, date of birth, social security/identification number and bank account numbers) via email, text or chat conversation.
- The sender requests a placement or processing fee.
- You are offered a job at Baxter after only a text or chat conversation.

What can I do to protect myself?

You can take several precautionary measures to protect yourself from recruitment fraud, including:

- **Verify the sender's email address and shared URLs.** Cyber criminals will often use modified email addresses or URLs or email addresses from free email services. For example, the email may come from baxter-inc.com, baxter-healthcare.com, baxter@gmail.com, rather than Baxter's authorized email extension—baxter.com—or Baxter's career site—jobs.baxter.com. Research the company's email address extension and URL using a search engine to verify its legitimacy.
- **Do not send money or provide credit card information to be considered for a job.** Legitimate employers, like Baxter, do not ask for money to have your application processed or to conduct a background check.
- **Do not share personal or financial data in response to an email request.** Do not share personal information via email, fax, or phone call with anyone purporting to be working for Baxter, because we will never ask for such information by such means. Personal or financial data may include bank account number, credit card number with security code, account username and password, date of birth, driver's license number and full social security/national identification number. If required, this information is only requested at the end of a thorough hiring process after a formal offer of employment has been made or an employment contract has been signed. At that point, this type of sensitive information can often be provided through a secure online system.
- **Be cautious of unsolicited offers of employment.** If you are offered a role with Baxter via email, a social media site such as LinkedIn, or text message, ask to speak to someone on the phone and capture their name, the company or agency they represent, their office location and contact details. If you are still

suspicious of the offer, complete this brief form to notify us of the suspected fraud and someone from our recruitment team will be in touch.

What should I do if I suspect I have been a victim of recruitment fraud?

If you suspect you are the victim of an online job-hunting scam by someone posing as a Baxter recruiter, employee or other agent, complete this form to notify us of the suspected fraud. A Baxter representative will be in touch after assessing the legitimacy of the reported incident.

For Job Seekers in the U.S.

The Federal Trade Commission, the United States' consumer protection agency, has published resources for detecting job scams. If you have concerns related to this issues, consider the following actions: 1) file a report with your local police department; 2) File a complaint with the Internet Crime Complaint Center; and/or 3) file a complaint with the U.S. Federal Trade Commission

For Jobs Seekers Outside the U.S.

Many countries have published resources for detecting job scams. We recommend you conduct an internet search for local resources and/or file a report with local authorities.