Beware of Fraudulent Recruiting Advertisements

We have become aware that imposters are using RVL Pharmaceuticals' name and reputation to engage in “phishing” scams seeking personal or confidential information.

More particularly, certain email addresses and domain names using "rvl" are not authorized by or associated with RVL Pharmaceuticals, and are known to be used for fraudulent employment schemes.

If you are applying for a job at RVL, 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 identity using the Internet and social media. These scammers frequently misappropriate and use a company’s logo, names and photographs of its staff, 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 RVL Pharmaceuticals to steal from their victims.

When communicating with RVL through digital media, please note:

- All RVL positions are posted to our official careers site hosted by ADP Workforce Now. This site can also be accessed through our RVLPharma.com site by selecting “Careers”.
- RVL Pharmaceuticals does post advertisements to positions on sites like Indeed and LinkedIn. However, be aware that when applying to the position, the links should redirect you to the RVL website – NOT 3rd party sites (like Fountain.com, Jora.com, Craigslist, ZipRecruiter, etc). Any such listings which take you to a 3rd party to complete the application are fraudulent.
- RVL Pharmaceuticals never requires any job applicants to pay money to anyone (RVL 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 our company in any way, and are likely seeking to defraud you.
- RVL only conducts job interviews in person, by telephone, and occasionally via Microsoft Teams or Webex, and never interviews job applicants through chats (like Wire or Google Hangouts), or through instant messaging systems. RVL does not permit our employees to send or receive work-related e-mails from personal accounts, and does not conduct job interviews by text/chat, or through Google Hangouts or other chat programs. 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 RVL and are likely seeking to defraud you.
- RVL's recruiting staff only sends email communications to job applicants from “@rvlpharma.com” email addresses and do not use email accounts such as Gmail or Yahoo for recruiting purposes. You should assume that any email claiming to be from RVL that does not have a “@rvlpharma.com” OR "@rvlpharmacy.com" address is fraudulent and is not from RVL.
- If you have any questions about the above or have concerns about a website or email communication concerning RVL Pharmaceuticals that you suspect may be fraudulent, please contact us at hr@rvlpharma.com.

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 RVL 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 “@rvlpharma.com” OR "@rvlpharmacy.com", such as “@rvlpharma.co,”, "@rvl.com", "@rvl.co", “@gmail.com,” “@yahoo.com,” “@outlook.com,” or another personal email account.
- The recruiting process asks for you to download a specific web or cell app in order to communicate with the recruitment team.
- 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).
- 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 chats or apps 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://www.fbi.gov/contact-us
- 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