

Job Scam Statement for UroGen.com/careers

Final Statement: Legal Approved Sep 7, 2022

### **Attention: Job Scam Alert**

UroGen has become aware of scams in which individuals who are not part of our company claim to represent UroGen in recruitment activities, including issuing fake offer letters. Please be aware that career opportunities are published only through UroGen's official communication channels. We will never ask for payments or fees from job applicants, and applicants will only be contacted by UroGen team members by phone or through an official UroGen email address ending in @urogen.com. Interviews with UroGen will never be conducted via Fleep, Google Hangouts, WhatsApp, or other social media platforms or apps. If you receive a suspicious email or job offer that claims to be on behalf of UroGen, do not provide any personal information or pay any fees. If you suspect any fraudulent recruitment activity by bad actors claiming to act for UroGen, please report it immediately to [Legal@urogen.com](mailto:Legal@urogen.com). Thank you.

Job seekers who have an interest in UroGen and any of its posted job positions should visit the "Work With Us" tab on the company's website, [www.urogen.com](http://www.urogen.com), or contact [hr@urogen.com](mailto:hr@urogen.com) for employment related inquiries.

Below is guidance from law enforcement that may help you protect yourself from similar fraudulent activities.

### **How to Spot a Scam**

- If the potential employer asks for payment upfront, your bank or credit card information, it's likely a scam.
- A job posting that shows up on internet job boards, but not the company's website may also indicate a scam.
- Hiring companies should not be asking jobseekers to make payments or do unorthodox things with their bank account or deposit checks.
- If someone from a company contacts you by phone ask if you can call them back after you verify the information.

### **How to Protect Yourself**

- Search for the company's website or contact information independently. Don't use the contact information provided to you by a stranger.
- If you find multiple websites for the same company or the web address is just a few letters off from an actual company website URL, it may have been spoofed.
- Never send money via wire transfer or a cash app to a potential employer you met online. You can also call your bank before agreeing to any transactions to give the bank a chance to flag a potential scam.

We wish you well. Be safe.