IMPORTANT INFORMATION

BEWARE OF FRAUDULENT RECRUITMENT ACTIVITY

Fraudulent recruitment activity is becoming more sophisticated and may apply to a range of scenarios. These schemes may be sent to an individual in a variety of formats, including e-mail, texts, messaging applications, social media or a letter. This type of fraud can also be perpetrated through online services with bogus websites with fraudulent domain name URLs, or even done through otherwise legitimate online job websites.

Wrongdoers may feature a company's name and logo without authority, falsely claiming that they represent the company and are interested in hiring individuals. Wrongdoers may even attempt to impersonate individuals who actually work for the company. These wrongdoers may offer fraudulent employment opportunities to individuals and often ask for sensitive personal and financial information as a part of their scheme.

Alvogen and Almatica condemn such fraudulent activity and take this issue very seriously. Below is information to help identify recruitment fraud and some steps you can take to protect yourself.

HOW TO IDENTIFY FRAUD

- Fraudulent recruitment e-mail correspondence is often sent from free web-based email accounts such as Gmail or Hotmail. We do not communicate with any potential job applicants through these web-based email services.
- Fraudulent recruitment messages may also arrive via messaging applications, such as Telegram. We do not communicate with any potential job applicants through such messaging applications.
- There is an early request for personal information or payment, or a request to cash a check.
- You may be referred to an organization that requests fees for processing certain documents, such as work permits, visa applications or the like.
- The perpetrators frequently (but not necessarily) use mobile or platform telephone numbers beginning with +44(0)70 instead of official company numbers.
- There is an insistence on urgency.

WHAT SHOULD I DO IF I BELIEVE I HAVE IDENTIFIED FRAUD?

DO

- Save messages from the perpetrator for further investigation, if necessary. Take screenshots if there is a possibility of deletion.
- Contact law enforcement and provide them will all information you may have from the perpetrator so that law enforcement can take any appropriate action.
- If you would like, you may send any relevant information to reportphishing@alvogen.com. We will strive to investigate the situation and take appropriate corrective action. Please note, any information or materials provided to us should not include any personal information (e.g. Social Security numbers, bank account details, etc.)

DO NOT

- Do not disclose your personal or financial details to anyone you do not know.
- Do not send any money to Alvogen or Almatica. We do not and will not ask for money transfers or payments.
- Do not engage in further communications if you believe the communications may be fraudulent.

For further information, the following webpage from the Federal Trade Commission may be useful in protecting yourself further:

https://www.consumer.ftc.gov/articles/0243-job-scams