FRANKLIN & MARSHALL COLLEGE

OFFICE OF STUDENT AND POST-GRADUATE DEVELOPMENT

Identifying Fraudulent Job Postings and Researching Companies

Fraudulent employers and opportunities can be difficult to spot. OSPGD looks for common red flags when we approve postings, and we encourage you to be vigilant and research opportunities as well.

The following red flags and actions, while not exhaustive, can serve as a reference as you gauge whether or not to apply to a posted job. Keep in mind that a red flag does not mean that a job posting or company is definitely fraudulent but rather, is an indication for you to proceed with caution, gather additional information, ask questions, and do more research.

COMMON RED FLAGS:

- The posting appears to be from a reputable, familiar company (often a Fortune 500 company) or even a well-known local establishment. However, the domain in the contact's email address does not match the domain used by representatives of the company. Be suspicious of personal email domains such as @live.com, @hotmail, @yahoo, or @gmail.
- The posting does not include a physical address, contact or company name.
- The website listed in the posting is not active, does not exist, or re-routes you to an unaffiliated website.
- The organization responds immediately after you submit your resume. Resumes are often reviewed by multiple individuals or not viewed until the posting has been closed. Note: This does not refer to an auto-response confirming that your resume has been received.
- The position requires an initial investment by you or for you to provide your credit card, bank or PayPal account numbers or other personal financial information.
- You receive a check from the organization or are offered a payment for the use of your bank account.
- The posting or correspondence contains spelling and/or grammatical errors.
- You are asked to provide a photo of yourself.
- The posting does not include job responsibilities and instead focuses on the money you can earn.
- Common job titles used in fraudulent postings include: Envelope Stuffers, Home-based Assembly Jobs, Online Surveys, or Check Writing and Processing.

ACTIONS YOU CAN TAKE:

- View the company website. Does it have an index that tells what the site is about or does it contain only information about the job you are interested in? Fraudulent employers may create quick, basic web pages that may seem legitimate at first look.
- Google the company name to see whether reported scams come up in the search (e.g. Acme Scam).
- Google the organization's and contact's phone number, fax number, and email address to ensure they are connected to an actual business.
- Google Map the physical address of the organization. If the street view image does not appear to be a business operation, then it may be a fraudulent address.
- Check the organization's rating with the Better Business Bureau (https://www.bbb.org/us/consumers/) or contact the Federal Trade Commission at 1-877-FTC-HELP (1-877-382-4357).

If you notice anything suspicious, do not apply to the opportunity, and email ospgd@fandm.edu to let us know. If you have been involved in a scam or fraudulent employer situation please contact OSPGD at (717) 358-4084 or F&M's Public Safety at (717) 358-3939.