FRAUDULENT EMPLOYERS:
HOW TO AVOID THEM AND WHAT TO DO IF YOU APPLY TO ONE

The Yeshiva University Career Center strives to serve as an excellent resource for employers to connect with YU students and alumni seeking internships, externships, and career related jobs. We allow employers to post jobs and allow students to access this information on our online job database, YU CareerLink (YUCL).

Regarding YUCL job postings: *YU does not endorse or recommend employers, and a posting does not constitute an endorsement or recommendation. The University explicitly makes no representations or guarantees about job listings or the accuracy of the information provided by the employer. The University is not responsible for safety, wages, working conditions, or any other aspect of off-campus employment without limitation. It is the responsibility of students to perform due diligence in researching employers when applying for or accepting private, off-campus employment and to thoroughly research the facts and reputation of each organization to which they are applying. Students should be prudent and use common sense and caution when applying for or accepting any position.*

Avoiding Fraudulent Employers

It is very important for you to educate yourself about potential scams. Fraudulent job postings may exist in an effort to take your money, personal information, or both. Please familiarize yourself with the following tips to help you evaluate job postings. These "red flags" in no way cover all possible instances of fraud. Therefore, please always use your own discretion when applying to a position or interacting with a potential employer.

Warning Signs

- Applicants are asked to pay a fee to obtain a job.
- The posting includes many spelling and grammatical errors.
- You are asked to provide a photo of yourself or provide personal, detailed information (marital status, age, weight, etc.).
- The position is for any of the following: Envelope Stuffers, Home-based Assembly Jobs, or Online Surveys.
- The job description focuses on the amount of money to be made.
- The salary is excessively high for a position of that type or for a job that requires minimal skills.
- Company's website doesn't look legitimate.
- Proceed with caution if it is difficult to find an address or an actual contact name. Be wary if the contact email address contains a non-business email domain (such as gmail.com) or is a personal email address. Check to make sure email address matches the domain used by others in the company.

Researching Possible Scams

Google the company name and the word "scam" or “hoax” and look at the results. You can also check to see if a company is legitimate through various websites:

- **Better Business Bureau**: http://www.bbb.org/
- **Chamber of Commerce**: http://www.uschamber.com/
- **Hoover’s**: http://www.hoovers.com/
- **White Pages**: http://www.whitepages.com/business

What You Should Never Do

- Never give your personal bank account, PayPal account, credit card information, or any other personal financial documentation to a new employer.
- Never agree to have funds or paychecks directly deposited into any accounts by a new employer (Arrangements for direct deposit or paycheck should be made during your first day or week of actual employment on site - not before.).
- Never purchase any products on behalf of the employer as part of your employment (such as Green Dot MoneyPaks, giftcards, phone cards, etc.).
- Never forward, transfer, or send by courier (i.e. FedEx, UPS) or "wire" any money to any employer, for any employer, or using your personal account(s).
- Never transfer money and retain a portion for payment.

If You Have Already Responded

As long as you did not include personal or financial information such as your social security number, any bank numbers, or a photo with your application, there is a low risk that your privacy would be compromised at this point. However, if you are contacted by the company, you should not fill out any additional paperwork, and we suggest you do ***not*** respond at all.

Next Steps If You Have Been Scammed

The Federal Trade Commission (FTC) offers the following instructions for students who have responded to fraudulent postings:

- Students should immediately contact the local police. The police are responsible for conducting an investigation (regardless of whether the scam artist is local or in another state).
- If you have sent money to a fraud employer: you should contact your bank or credit card company immediately to close the account and dispute the charges.
- If the incident occurred completely over the Internet, you should file an incident report at http://www.cybercrime.gov/ or by calling the FTC at: 1-877-FTC-HELP (1-877-382-4357).

Contact Us Immediately

Any time you have concerns about the legitimacy of an employer or a job posting on YUCL, report your concerns to the YU Career Center at 646-592-4090 or careercenter@yu.edu. A member of our staff will follow up.