Protecting Yourself from Fraudulent Employers

What is a Fraudulent Employer?
Have you been offered a position for $3,000 per day? More than likely, you’ve come across a fraudulent job posting. Unfortunately in today’s market, fraudulent postings are becoming more prevalent, whether you’re finding jobs through a CSB/SJU career or experiential learning link site or a non-campus sponsored site. In an effort to help you identify potential warning signs, we ask that you please review the list below and use it when evaluating job and internship postings and emails you receive.

Fraudulent Posting Red Flags to Watch For:
- Those that require you to provide your credit card, bank account numbers, other personal financial documentation, or one that requires an initial investment, such as a payment by wire service or courier, or those that require you to invest in products at the outset.
- The posting appears to be from a reputable, familiar company (often a Fortune 500); however, the domain in the contact’s email address does not match the domain used by representatives of the company (this is typically easy to determine from the company's website). Another way to validate is to check the open positions on the company’s website.
- The contact email address contains the domain @live.com.
- The posting includes many spelling and grammatical errors.
- The position initially appears as a traditional job, but upon further research, it sounds more like an independent contractor opportunity.
- You receive an unexpectedly large check (checks are typically slightly less than $500, generally sent or deposited on Fridays).
- You are asked to provide a photo of yourself.
- The position is for any of the following: Envelope Stuffers, Home-based Assembly Jobs, Online Surveys.
- The posting neglects to mention what the responsibilities of the job actually are. Instead, the description focuses on the amount of money to be made.
- The employer responds to you immediately after you submit your resume. Typically, resumes sent to an employer are reviewed by multiple individuals, or not viewed until the posting has closed.
  - Note: this does not include an auto-response you may receive from the employer once you have sent your resume.
- The position indicates a “first year compensation" that is in high excess to the average compensation for that position type.
- Watch for anonymity. If it is difficult to find an address, actual contact, company name, etc. - this is cause to proceed with caution. Fraud postings are illegal, so scammers will try to keep themselves well-hidden. Oftentimes a check of the business name with the Better Business Bureau is a good place to start your detective work.
- The salary range listed is very wide (i.e. "employees can earn from $40K - $80K the first year!")
- When you Google the company name and the word "scam" (i.e., Acme Company Scam), the results show several scam reports concerning this company. Another source for scam reports is: http://www.ripoffreport.com.
- Google the employer’s phone number, fax number and/or email address. If it does not appear connected to an actual business organization, this is a red flag. You can use the Better Business Bureau (http://www.bbb.org/us/consumers/), Hoovers (http://www.hoovers.com/) and AT&T’s Anywho (http://www.anywho.com/) to verify organizations.
- The employer contacts you by phone; however there is no way to call them back. The number is not available.

Let us know:
If you see a position in our system that you believe may be a scam, please notify our office immediately! If you receive an email that meets any of the above criteria, do not respond - delete the email.

Additional Resources:
http://www.bbb.org/us/article/5392
http://jobsearch.about.com/od/jobsearchscams/qt/scamexamples.htm

If you have any questions or concerns about fraudulent postings, please contact
Experiential Learning & Community Engagement:
Laura Hammond, Assistant Director
P: (320)-363-5300 or E: lhammond@csbsju.edu

Acknowledgment: We acknowledge Hamline University’s Office of Career Services, whose Fraudulent Posting Handout served as a guide for these materials.