

Pitzer College Career Services
Fraudulent Job Posting Warning and Information

Fraudulent Job Postings Statement

Opportunities posted on ClaremontConnect may or may not be reviewed prior to posting and The Claremont Colleges have no control over the quality, safety or legalities of said opportunities. The approving college cannot be held responsible and/or liable for any damages from the information contained in, or requested by, the opportunities found in the Handshake network. Users are urged to review opportunities on a case by case basis and use caution and common sense before applying.

Fraudulent Job Postings Warning

Pitzer Career Services and the Career Centers of The Claremont Colleges work hard to keep fraudulent jobs and employers out of ClaremontConnect; however, fraudulent employers and jobs sometimes make it through our screening process. We ask that you perform your due diligence and research employers and job postings to protect yourself from employment scams.

Below are some of the common red flags that indicate a job posting might be a scam. If you become suspicious of a posting in ClaremontConnect or a communication from an employer, please email careerservices@pitzer.edu or call Pitzer Career Services at 909.621.8519 so that we can investigate and take appropriate action.

If you feel you are the victim of an employment scam please contact the local police. If you provided your credit card number, banking information or money to a fraudulent employer please contact your bank and credit card company to close your accounts and dispute the charges.

If the incident occurred completely over the internet, you should file an incident report with The United States Department of Justice (www.cybercrime.gov) and the Federal Trade Commission (<http://www.ftc.gov>).

Red Flags

The following “red flags” are general markers to help you conduct a safer job search and protect your identity. These “red flags” do not cover all possible instances of fraud. Therefore, please always use your own discretion when applying to a position or interacting with a potential employer.

- You must provide your credit card, bank account numbers, or other personal financial documentation.
- The posting appears to be from a reputable, familiar company (often a Fortune 500), yet, 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 position requires an initial investment, such as a payment by wire service or courier.
- The posting includes many spelling and grammatical errors.
- The position initially appears as a traditional job. Upon further research, it sounds more like an independent contractor opportunity. Debbie Kaylor, Career Center Director at Boise State

Thanks to the Career Services Offices at Rutgers, USC, Azusa Pacific, UC Santa Barbara, and Claremont Graduate University for compiling the information on red flags and avoiding job scams.

University, discusses this further in her blog posting at:

<http://www.bsucareercenter.blogspot.com/>.

- You are offered a large payment or reward in exchange for allowing the use of your bank account (often for depositing checks or transferring money).
- 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 the responsibilities of the job. 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 excess of the average compensation for that position type.
- The company's website does not have an index that tells you what the site is about. It contains information only about the job in which you are interested. Scammers often create quick, basic web pages that seem legitimate at first glance.
- Anonymity - If it is difficult to find an address, actual contact, company name, etc. Fraudulent postings are illegal, so scammers will try to keep themselves well-hidden.
- The salary range listed is very wide (e.g., "employees can earn from \$40K - \$80K the first year!").
- An internet search of the company name shows several scam reports concerning this company (e.g., Acme Company Scam). Another source for scam reports is: <http://www.ripoffreport.com>.
- An internet search of the employer's phone number, fax number and/or email address does not appear to connect these to an actual business organization. The Better Business Bureau (<http://www.bbb.org/us/consumers/>) and AT&T's Anywho (<http://www.anywho.com/>) are possible sites to conduct these searches.
- The employer contacts you by phone, but there is no way to call them back (the number is not available).
- The employer tells you that they do not have an office set up in your area and will need you to help them get it up and running (these postings often include a request for your banking information, supposedly to help the employer make transactions).
- The jobs often appear easy and convenient ways to make money with very little effort. Fraudulent job postings try to take your money, personal information, or both.

Core Essentials to Avoiding a Job Posting Scam

- Do not give your personal bank account, PayPal account, or credit card information to a new employer.

Thanks to the Career Services Offices at Rutgers, USC, Azusa Pacific, UC Santa Barbara, and Claremont Graduate University for compiling the information on red flags and avoiding job scams.

- Do not 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.)
- Do not forward, transfer or send by courier (i.e. FedEx, UPS), or “wire” any money to any employer or for any employer, using your personal account(s).
- Do not transfer money and retain a portion for payment.
- Do not respond to suspicious and/or “too good to be true” unsolicited job emails.

In general, applicants do not pay a fee to obtain a job (but there are some rare exceptions – so be careful, and consult with a professional at Career Services first).