

## EXCERPT FROM: FRAUDULENT EMPLOYERS: TIPS FOR CAREER CENTERS AND STUDENTS

### STUDENTS: RED FLAGS TO CONSIDER

Fraudulent employers are phishing for the unsuspecting, including you. Be aware of what you share and post online. If you feel uncomfortable or are not sure about certain organizations or individuals claiming to represent an employer, talk to your career center.

What are some “red flags” students should be aware of to avoid fraudulent employers when using online job and internship sites?

### ADDITIONAL RESOURCES FROM THE FBI

- [Internet Crime Complaint Center](#)
- [Employment Scam Targeting College Students Remains Prevalent](#)
- [File an Internet crime complaint with the FBI.](#)
- [FBI fraud alert poster](#)

### Requests for financial/personal information are red flags. Here are some examples:

- You must provide your credit card or bank account numbers or other personal financial documentation. Do NOT give out any financial information at any point during your job-search and hiring process.
- You are asked to provide your social security and driver’s license information in the initial application. Personal information should never be asked during the initial application process.
- The representative tells you that the organization does not have an office set up in your area and will need you to help get the office up and running. This scam often includes a request for your banking information, supposedly to help the employer make transactions.
- The position requires an initial investment, such as a payment by wire service or courier.
- 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 to deposit into your bank account.
- Remember: Never process ANY financial transactions. For example, some organizations offer opportunities to “make quick money.” They will offer a “one-day only special.” Their intent is to defraud you by sending or wiring money to your bank account. They will ask you to cash the check or send the monies to other accounts. Once your bank or financial institution processes the scammer’s check or financial request, you may be informed the monies are invalid or “not real.” In the meantime, you are held responsible for the funds the bank has sent at your direction to other accounts.

### An unusual salary is a red flag. Some typical examples include:

- The position indicates a "first-year compensation" that is in high excess to the average compensation for that position type.
- The salary range listed is very wide, e.g., "employees can earn from \$40K - \$80K the first year."
- The position initially appears as a traditional job. Upon further research, it sounds more like an independent contractor opportunity.

### Websites and emails can signal a problem. For example:

- The posting appears to be from a reputable, familiar organization—often a Fortune 500. Yet, the email handle in the contact's email address does not match the domain used by representatives of the organization; this is typically easy to determine from the organization's website. Another way to validate is to check the open positions on the organization's website by checking their careers/jobs webpage.
- The contact email address contains the domain @live.com or an @ that is not affiliated with the organization. Examples: @gmail, @yahoo, @hotmail. If this is the case, then verify that the email address matches what is found on the organization's website.
- You receive unsolicited email that is not specifically directed to you. Spammers/scammers can obtain student emails fairly easily. If the unsolicited email references a referral from your career center, contact your career center to verify the employer.
- You are directed to a very basic website. Does the organization's website have an index that tells you what the site is about; or does it contain information only about the job in which you are interested? Scammers often create basic webpages that seem legitimate at first glance.

### Other red flags include:

- The employer is hard to find. Scammers will try to keep themselves well hidden. Watch for anonymity. If it is difficult to find an address, actual contact, organization name, or similar information, this is cause to proceed with caution.
- The employer contacts you by phone, but there is no way to call the representative back, i.e., the number is not available.
- 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 interview is conducted online or over the phone, and an offer is given almost immediately.
- The posting includes many spelling and grammatical errors.
- The posting neglects to mention the responsibilities of the job. Instead, the description focuses on the amount of money to be made.
- When you Google the organization name and the results include spam reports about the organization. Another source for scam reports is [www.ripoffreport.com](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](#), [Hoovers](#), and [Anywho](#) to verify organizations.
  - You can also use social media to research each employer, e.g., Facebook, Twitter, Snapchat, and LinkedIn. Research the organization on websites such as Glassdoor.com for feedback and complaints.

**Bottom line: If you have any questions or suspicions, contact your career center or campus police before pursuing any opportunity. If it sounds too good to be true, it probably is.**

*\* Note: The recommendations contained herein do not constitute legal advice and are not an exhaustive list. You are encouraged to speak to your legal counsel to discuss these issues more fully. A career center should also include a disclaimer that states that it does not ensure the viability of any employer and that it does not guarantee that all employers are reviewed.*

*Reviewed and updated by the 2020 Principles for Ethical Professional Practice Committee.*