

Fraudulent Job Postings

The Practice Department makes every effort to screen employers and job postings on Practice Lab. However, fraudulent jobs can be difficult to spot at first, and students are encouraged to exercise caution and use common sense when searching for and applying to jobs.

How can you tell if a job might be fraudulent? Here are a few red flags:

- You are asked to provide personal information, such as Social Security Number, bank account or credit card numbers, copies of your passport and/or license, and other personal and financial documentation.
- You are offered a job without ever having met your employer.
- The posting includes many spelling and grammatical errors.
- You are asked to provide a photo of yourself.
- You experience repeated difficulties in attempting to identify or contact the recruiter [i.e. the number provided always leads to a generic voicemail system].
- The contact's email address does not match up to the company's website domain [i.e. a well-known company sends an email from an AOL, Yahoo, or Gmail account].
- Promises a large amount of money in return for little work.
- You are asked to wire or transfer money from one account to another.
- You receive an unexpected check in the mail prior to having formalized an offer or even met with the employer.
- The job description is vague or unclear, and the focus is more on the money you will make.
- It sounds too good to be true – because, it usually is!

If you are suspicious of a posting, end communication with the employer immediately and contact the Practice Department at practice@the-bac.edu or call 617.585.0145.

If you have released personal information, such as bank account or credit card numbers, contact your bank or credit card company immediately.

If a fraudulent exchange occurred completely over the Internet, you can file an incident report with the [Federal Trade Commission Cyber Crime Division](#) or call the FTC at: 1-877-FTC-HELP (1-877-382-4357).