Handshake & Other Third-Party Opportunity Databases Disclaimer

The Augsburg University Strommen Career & Internship Center advises students to treat Handshake, a third-party platform, with the same level of caution that they would give to any database offering opportunities. Because of the vast volume of job and internship postings on Handshake, the University neither endorses nor makes any claims about the accuracy of descriptions of employers or their postings.

The University is not responsible for the working conditions, safety, compensation, or any other aspect of opportunities resulting from postings on Handshake (or any other source). It is the responsibility of the student/applicant, when applying for or accepting an offer, to perform due diligence in researching employers. Furthermore, neither the college nor the Strommen Center is responsible for any employer's hiring decisions or practices, including rescinded offers. We strongly encourage students to use their best judgement when reviewing Handshake postings, employers, and job/internship work sites. We encourage students to contact the Strommen Center with any questions about any information posted in Handshake or to report potential fraud, misinformation or inaccuracies in the system.

<u>Identifying Fraudulent Job and Internship Postings</u>
Unfortunately, not every job posting is a genuine opportunity. Scammers know that job offers are a powerful tool for harvesting personal information, and so you need to know how to distinguish legitimate job postings from scam attempts. If you experience anything unusual about a job posting in Handshake, please contact the Strommen Center as soon as possible.

Basic Tips:

- When in doubt, look for the job posting on the company's official website. Much like phishing emails, scam job postings often capitalize on well-known companies' names and images. Type the company's name into Google (don't follow links from the suspicious posting, which could take you to a cosmetically similar page) and check the employment page to be sure that the opening is genuine. Calling the company in question (again, using publicly available contact information) is another good strategy.
- Don't provide financial information or your Social Security number! Legitimate employers won't ask for your bank account details or your SSN, and scammers will use this information for nefarious purposes.

- Do not send money! Legitimate employers will not ask you to wire money or pay for services. The one exception to this general rule would be a request from a search firm/headhunter, but even then, the rule of thumb is to avoid any search firm that asks you, the candidate, for money.
- If you're posting your resume online where it can be accessed by anyone, leave out personal information like specific details about past employers and your date of birth.
- If a job sounds too good to be true, *it almost certainly is.*

The "red flags" below are examples of strong warning signs that indicate probable fraudulent or unscrupulous employers. If you see any of these signs, you should cease communication and engagement immediately, and report the interaction to the Strommen Career & Internship Center.

- The same warning signs that signal fraudulent emails and websites: bad grammar and spelling, requests for personal information, and difficulty contacting or identifying the employer or organization posting are all clear signs of trouble
- You are contacted by phone, and the number is not available
- Vague descriptions that focus on money rather than the job
- Email domain (that's the @xyzcorp.com part of the address) that doesn't match the company's official website's domain
- Email domain of a free provider is used, such as: live.com, gmail.com, hotmail.com, etc. (With the possible exception of very new ventures such as start-ups, legitimate companies almost always have their own email systems.)
- Websites that have information only on the job you're applying for rather than about the company in general
- Requests for an initial investment
- Requests for bank account access
- Requests for payment or transfer of money.

What if I'm already involved in a scam?

- Immediately contact the local police and the Strommen Career and Internship Center. 612-330-1148 or email careers@augsburg.edu
- If necessary, get in touch with your bank or credit card company and dispute any fraudulent activity immediately.
- If the scam happened online, file a report with the FTC's cybercrime division

*Modified with approval from St. Olaf College, Piper Career Center