



OFFICE of PRIVATE SECTOR

ACADEMIA ENGAGEMENT REPORT (AER)

ACADEMIA

26 August 2022

AER 220826007

Fraudulent Employment Scheme Targeting University Students with the Potential for Causing Financial Loss

References in this Academia product to any specific commercial product, process, or service or the use of any corporate name herein is for informational purposes only and does not constitute an endorsement, recommendation, or disparagement of that product, process, service, or corporation on behalf of the FBI.

The FBI San Francisco Field Office, in coordination with the Office of Private Sector (OPS), prepared this AER to inform academia partners of a fraudulent employment scheme targeting university students. The purpose of this AER is to alert universities of this scheme to help prevent additional students from becoming victims. As part of this fraudulent employment scheme, criminal actors, purporting to be professors, contact students and offer employment opportunities. The fraudulent employment scheme leaves students who are seeking employment and/or career enhancing opportunities vulnerable to financial loss.

- In June 2022, a Massachusetts university student was contacted by an unknown individual believed to be a university professor offering a role working on a project as a research assistant. After the student accepted the job, the student received a check via email to pay for job supplies and subsequently deposited the check. The student received instructions to send half the amount of the check to an account via an electronic payment. After sending the funds, the student was directed to send the second half of the amount of the check to a different account. The student did not send the second amount of the check as instructed. The student also reported the deposited check was returned.
- In April 2022, a California university reported that students at the university had been defrauded by fake job listings. In these job listings, individuals pretended to be professors and solicited gift cards from the students.
- In April 2022, an Illinois university student received an email advertising a remote research assistant position open to any student at the university. After the student accepted the job, the student received a check via email to pay for supplies. The student was directed to send the amount of the check to an email address via a payment app. After the student sent the amount of the check, the bank determined this was fraud.
- In July 2021, an individual purporting to be a university professor contacted two California university students via email regarding virtual research assistant jobs at the university. The students received emails, purportedly from the university's human resources department, verifying the jobs. After the students accepted the jobs, the students were directed to purchase items needed for the positions. The students were told to send funds to a sales representative via an electronic payment system. Both students received checks via email from what appeared to be a legitimate university payroll accountant; however, the bank determined the checks were fake.







The FBI recommends alerting students and professors to be wary of unsolicited job opportunities. If offered a job from a university employee, the student should contact that university employee through official channels. Additional tips can be found on the Federal Trade Commission's website at <https://consumer.ftc.gov/articles/job-scams>. If your students, professors, or other university employees have been a victim of this scam, please report the incident to the Internet Crime Complaint Center (www.ic3.gov) and local law enforcement.

OPS's Information Sharing and Analysis Unit disseminated this AER. Direct any requests and questions to your FBI Private Sector Coordinator at your local FBI Field Office: <https://www.fbi.gov/contact-us/field-offices>.



Traffic Light Protocol (TLP) Definitions

Color	When should it be used?	How may it be shared?
<p>TLP:RED</p>  <p>Not for disclosure, restricted to participants only.</p>	<p>Sources may use TLP:RED when information cannot be effectively acted upon by additional parties, and could lead to impacts on a party's privacy, reputation, or operations if misused.</p>	<p>Recipients may not share TLP:RED information with any parties outside of the specific exchange, meeting, or conversation in which it was originally disclosed. In the context of a meeting, for example, TLP:RED information is limited to those present at the meeting. In most circumstances, TLP:RED should be exchanged verbally or in person.</p>
<p>TLP:AMBER</p>  <p>Limited disclosure, restricted to participants' organizations.</p>	<p>Sources may use TLP:AMBER when information requires support to be effectively acted upon, yet carries risks to privacy, reputation, or operations if shared outside of the organizations involved.</p>	<p>Recipients may only share TLP:AMBER information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm. Sources are at liberty to specify additional intended limits of the sharing; these must be adhered to.</p>
<p>TLP:GREEN</p>  <p>Limited disclosure, restricted to the community.</p>	<p>Sources may use TLP:GREEN when information is useful for the awareness of all participating organizations as well as with peers within the broader community or sector.</p>	<p>Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels. Information in this category can be circulated widely within a particular community. TLP:GREEN information may not be released outside of the community.</p>
<p>TLP:WHITE</p>  <p>Disclosure is not limited.</p>	<p>Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release.</p>	<p>Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.</p>