Public Service Announcement

FEDERAL BUREAU OF INVESTIGATION

January 18, 2017

Alert Number
I-011817-PSA

Questions regarding this PSA should be directed to your local **FBI Field Office**.

Local Field Office Locations:
www.fbi.gov/contact-us/field

EMPLOYMENT SCAM TARGETING COLLEGE STUDENTS REMAINS PREVALENT

College students across the United States continue to be targeted in a common employment scam. Scammers advertise phony job opportunities on college employment websites, and/or students receive e-mails on their school accounts recruiting them for fictitious positions. This "employment" results in a financial loss for participating students.

How the scam works:

- Scammers post online job advertisements soliciting college students for administrative positions.
- The student employee receives counterfeit checks in the mail or via e-mail and is instructed to deposit the checks into their personal checking account.
- The scammer then directs the student to withdraw the funds from their checking account and send a portion, via wire transfer, to another individual. Often, the transfer of funds is to a "vendor", purportedly for equipment, materials, or software necessary for the job.
- Subsequently, the checks are confirmed to be fraudulent by the bank.

The following are some examples of the employment scam e-mails:

"You will need some materials/software and also a time tracker to commence your training and orientation and also you need the software to get started with work. The funds for the software will be provided for you by the company via check. Make sure you use them as instructed for the software and I will refer you to the vendor you are to purchase them from, okay."

"I have forwarded your start-up progress report to the HR Dept. and they will be facilitating your start-up funds with which you will be getting your working equipment from vendors and getting started with training."

"Enclosed is your first check. Please cash the check, take $300 out as your pay, and send the rest to the vendor for supplies."

Consequences of participating in this scam:

- The student's bank account may be closed due to fraudulent activity and a report could be filed by the bank with a credit bureau or law enforcement agency.
- The student is responsible for reimbursing the bank the amount of the counterfeit checks.
- The scamming incident could adversely affect the student's credit record.
- The scammers often obtain personal information from the student while posing as their employer, leaving them vulnerable to identity theft.
- Scammers seeking to acquire funds through fraudulent methods could potentially utilize the money to fund illicit criminal or terrorist activity.

Tips on how to protect yourself from this scam:

- Never accept a job that requires depositing checks into your account or wiring portions to other individuals or accounts.
- Many of the scammers who send these messages are not native English speakers. Look for poor use of the English language in e-mails such as incorrect grammar, capitalization, and tenses.
- Forward suspicious e-mails to the college's IT personnel and report to the FBI. Tell your friends to be on the lookout for the scam.

If you have been a victim of this scam or any other Internet-related scam, you may file a complaint with the FBI's Internet Crime Complaint Center at www.IC3.gov and notify your campus police.

The IC3 produced a PSA in May 2014 titled "Cyber-Related Scams Targeting Universities, Employees, and Students," which mentioned this type of scam. This PSA can be viewed at https://www.ic3.gov/media/2014/140505.aspx.