IC3 PUBLIC SERVICE ANNOUNCEMENT
FEDERAL BUREAU OF INVESTIGATION

13 January 2015

Alert Number
I-011315a-PSA

FBI Warns of Fictitious 'Work-from-home' Scam Targeting University Students

College students across the United States have been targeted to participate in work-from-home scams. Students have been receiving e-mails to their school accounts recruiting them for payroll and/or human resource positions with fictitious companies. The "position" simply requires the student to provide his/her bank account number to receive a deposit and then transfer a portion of the funds to another bank account. Unbeknownst to the student, the other account is involved in the scam that the student has now helped perpetrate. The funds the student receives and is directed elsewhere have been stolen by cyber criminals. Participating in the scam is a crime and could lead to the student's bank account being closed due to fraudulent activity or federal charges.

Here's how the scam works:

- The student is asked to provide his/her bank account credentials under the guise of setting up direct deposit for his/her pay.
- The scammers will add the student's bank account to a victim employee's direct deposit information to redirect the victim's payroll deposit to the student's account.
- The student will receive the payroll deposit from the victim's employer in the victim's name.
- The student will be directed to withdraw funds from the account and send a portion of the deposit, via wire transfer, to other individuals involved in the scam.

Consequences of Participating in the Scam:

- The student's bank account will be identified by law enforcement as being involved in the fraud.
- The victim employee has his/her pay stolen by the scammers utilizing the student's bank account.
- Without the student's participation, the scam could not be perpetrated, so he/she facilitated the theft of the paycheck.
- The student could be arrested and prosecuted in federal court. A criminal record will stay with the student for the rest of his/her life and will have to be divulged on future job applications, which could prevent the student from beomg hired.
- The student's bank account may be closed due to fraudulent activity and a report could be filed by the bank.
- This could adversely affect the student's credit record.

IC3 PUBLIC SERVICE ANNOUNCEMENT

FEDERAL BUREAU OF INVESTIGATION

Tips on how to Protect Yourself from this Scam:

- If a job offer sounds too good to be true, it probably is.
- Never accept a job that requires the depositing of funds into your account and wiring them to different accounts.
- Look for poor use of the English language in e-mails such as incorrect grammar, capitalization, and tenses. Many of the scammers who send these messages are not native English speakers.
- Never provide credentials of any kind such as bank account information, login names, passwords, or any other identifying information in response to a recruitment e-mail.
- Forward these e-mails to the university's IT personnel and tell your friends to be on the lookout for the scam.

If you have been a victim of this scam, you may file a complaint with the FBI's Internet Crime Complaint Center at www.ic3.gov. Please reference this PSA number in your complaint.

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