# Public Service Announcement

FEDERAL BUREAU OF INVESTIGATION

July 2, 2010

## CLAIMS OF BEING STRANDED SWINDLES CONSUMERS OUT OF THOUSANDS OF DOLLARS

The IC3 continues to receive reports of individuals' e-mail or social networking accounts being compromised and used in a social engineering scam to swindle consumers out of thousands of dollars. Portraying to be the victim, the hacker uses the victim's account to send a notice to their contacts. The notice claims the victim is in immediate need of money due to being robbed of their credit cards, passport, money, and cell phone; leaving them stranded in London or some other location. Some claim they only have a few days to pay their hotel bill and promise to reimburse upon their return home. A sense of urgency to help their friend/contact may cause the recipient to fail to validate the claim, increasing the likelihood of them falling for this scam.

If you receive a similar notice and are not sure it is a scam, you should always verify the information before sending any money.

If you have been a victim of this type of scam or any other Cyber crime, you can report it to the IC3 website at: www.IC3.gov. The IC3 complaint database links complaints for potential referral to the appropriate law enforcement agency for case consideration. Complaint information is also used to identity emerging trends and patterns.