Fraud Advisory for **Consumers**
Involvement in Criminal Activity through Work from Home Scams

This product was created as part of a joint effort between the United States Secret Service, the Federal Bureau of Investigation, the Internet Crime Complaint Center (IC3) and the Financial Services Information Sharing and Analysis Center (FS-ISAC).

Consumers continue to lose money from work-from-home scams that assist cyber criminals move stolen funds. Worse yet, due to their deliberate or unknowing participation in the scams, these individuals may face criminal charges. Work-from-home scam victims are often recruited by organized cyber criminals through newspaper ads, online employment services, unsolicited emails or "spam",[1] and social networking sites advertising work-from-home opportunities. Once recruited, however, rather than becoming an employee of a legitimate business, the consumer is actually a "mule" for cyber criminals who use the consumer's or other victim's accounts to steal and launder money. In addition, the consumer's own identity or account may be compromised by the cyber criminals.

Example of a Work-From-Home Scheme:

- An individual applies for a position as a rebate or payments processor[2] through an online job site or through an unsolicited email.
- As a new employee, the individual is asked to provide his/her bank account information to his/her employer or to establish a new account using information provided by the employer.
- Funds are deposited into the account that the employee is instructed to wire to a third (often international) account. The employee is instructed to deduct a percentage of the wired amount as their commission.
- However, rather than processing rebates or processing payments, the individual is actually participating in a criminal activity by laundering stolen funds through his/her own account or a newly established account.

In February 2010, the U.S. Federal Trade Commission (FTC) coordinated with state law enforcement officials and other federal agencies to announce a sweeping crack down on job and work-from-home fraud schemes fueled by the economic downturn. Individuals who are knowing or unknowing participants in this type of scheme could be prosecuted.

[1] Cyber criminals may also spoof a legitimate business to entice you into opening the email, which may contain a fraudulent application for information or malware.
[2] Other common job titles for these schemes include trading partner or currency trader.

Protect Yourself:

- Be wary of work-from-home opportunities. Research the legitimacy of the company through the Better Business Bureau[3] (for US-based companies) or WHOIS/Domain Tools[4] (for international companies) before providing personal or account information and/or agreeing to work for them. In addition, TrustedSource.org can help you identify companies that may be maliciously sending spam based on the volume of email sent from their Internet Protocol (IP)[5] addresses. See also the FTC's recommendations[6].
- Be cautious about any opportunities offering the chance to work from home with very little work or prior experience. Remember: if it looks too good to be true, it usually is.
- Never pay for the privilege of working for an employer. Be suspicious of opportunities that require you to pay for things up front, such as supplies and other materials.
- Never give your bank account details to anyone unless you know and trust them.
- If you think you may be a victim of one of these scams, contact your financial institution immediately. Report any suspicious work-from-home offers or activities to the Internet Crime Complaint Center (IC3)[7] at http://www.ic3.gov/default.aspx.

For more information, visit:

- PhishBucket.org, a nonprofit organization dedicated to protecting job seekers from fraudulent job offers.
- OnGuardOnline.org. Sponsored by the FTC, this site provides practical tips from the federal government and the technology industry to help you be on guard against Internet fraud, secure your computer, and protect your personal information.
- Better Business Bureau, http://www.bbb.org/us/article/work-at-home-schemes-408.

This advisory was created through a collaborative cross-industry effort to protect consumers and businesses against account takeovers. Led by the Financial Services Information Sharing and Analysis Center (FS-ISAC), contributors include more than 30 of the largest financial institutions in the U.S., industry associations including the American Bankers Association (ABA), NACHA - The Electronic Payments Association, BITS/The Financial Services Roundtable; and federal regulatory and law enforcement agencies.

[3] http://www.bbb.org/
[4] http://www.domaintools.com/
[5] An IP address identifies the company's website host or network interface and location.
[6] http://www.onguardonline.gov/topics/email-scams.aspx#3
[7] The IC3 is a partnership between the Federal Bureau of Investigation (FBI), the National White Collar Crime Center (NW3C), and the Bureau of Justice Assistance (BJA).