



**INTERNET CRIME COMPLAINT CENTER'S (IC3)
SCAM ALERTS
MAY 10, 2011**



This report, which is based upon information from law enforcement and complaints submitted to the IC3, details recent cyber crime trends and new twists to previously-existing cyber scams.

JOB SCAM USED TO RESHIP MERCHANDISE TO RUSSIA

In the reshipping scam, subjects hire individuals to receive, readdress, and forward or "reship" packages to addresses generally in the United Kingdom or Nigeria with recent schemes using addresses in Russia. Subjects purchase the reshipped merchandise with compromised credit cards. Some reshippers recognize the scam and are complicit in perpetuating the fraud, while other reshippers appear to be unaware of the scam. Often, reshippers realize the fraud upon receiving calls from the companies that sold the merchandise or from the owners of the stolen credit card numbers.

In a new version of this scam, subjects hire individuals as "Gift Wrapper Associates" to receive and gift-wrap merchandise and ship it to given addresses. Recent complainants reported they had responded to Craigslist ads, while others were contacted by email, possibly as a result of a resume they had posted online. Additionally, the complainants reportedly participated in phone interviews as part of the hiring process and were required to provide personally identifiable information (PII).

Subjects provide reshippers the necessary supplies to wrap the merchandise, such as boxes, wrapping paper, tape, ribbons, and bows. The victims' PII gathered during the application process could potentially be used to obtain credit for other fraudulent purchases or to conduct other criminal activities. Such unauthorized use of PII often occurs in many types of identity theft-related scams such as other work-at-home, phishing, and various counterfeit check scams.

COUNTERFEIT CHECK SCAM TARGETING REALTORS AND REAL ESTATE ATTORNEYS

Through the years, the IC3 has continued to receive complaints reporting counterfeit check scams. In this particular scam, subjects attempt to convince unwitting victims to cash checks or money orders and wire a portion of the funds overseas. After wiring the funds, the victim discovers that the check was fraudulent and is held responsible for the check amount.

One of the latest counterfeit check scams targets realtors and real estate attorneys. International subjects have been contacting U.S. realtors and real estate attorneys, claiming to be interested in purchasing property in the U.S. Subjects request a properties listing from realtors, indicating their intent to pay cash for the real property. Subjects then ask the realtor to provide a local attorney to handle the purchase and conduct the closing. Upon negotiating the price, the real estate attorneys received checks that were often written for hundreds of thousands of USD. Once the check had been deposited, but before it cleared, the subject provided a reason for a portion of the funds to be wired to his account. Often in these scams, victims are not aware that the checks are from legitimate businesses' accounts, fraudulently obtained by the subjects.

In January 2010, the IC3 released a [Public Service Announcement](#) detailing a similar counterfeit check scam, which targeted law firms in the U.S.