# INTERNET CRIME COMPLAINT CENTER'S (IC3)
# SCAM ALERTS
# SEPTEMBER 19, 2012

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.

## TRIANGLE CREDIT CARD FRAUD

Triangle Credit Card Fraud is a common scam known to affect many on-line merchants. It has been called "Triangle Credit Card Fraud" because there are three primary parties involved or impacted by the scam.

The first party is the fraudster who acts as a seller on a popular auction or marketplace site. The fraudster "sells" a product to the second party, the buyer that knows nothing about the scam. The buyer pays the seller for the product or service. The seller then needs to deliver the product or service to the buyer and does so by placing an order with the manufacturer of the product or service to the buyer and does so by placing an order with the manufacturer of the product or service, the third party. That order will contain the buyer's information for shipping and stolen credit card information for billing. When the company receives the order, the billing and shipping information is all legitimate, thus it looks like an order being placed as a gift, so the company delivers the product or service.

When the card holder finds a fraudulent charge on their card, they may file a dispute with the credit card company resulting in a chargeback for the company. This scheme is often much more complex as it is often led by overseas criminals who recruit established sellers (often referred to as mules) on auction or marketplace sites to "sell" the products. Once a sale is completed, the mule will forward the buyer information and the bulk of the money to the fraudster to place the fraudulent order. Once a mule becomes trusted, they are often allowed to recruit other mules, leading to a complex pyramid of fraudsters and mules.

Through the on-line merchant community, many companies have been made aware of this scheme and have had great successes with stopping the illegal activity using fraud prevention and detection solutions as well as successful criminal prosecutions.

## NEW TWIST TO THE WORK-AT-HOME SCHEME

The IC3 has previously reported on work-at-home schemes where victims advised they applied for employment through on-line resumes. The alleged employers used the names of well-known financial institutions and industry agencies to lure their victims into the scheme. The potential employees were contacted via e-mail and interviewed for various positions using Yahoo! Instant Messenger.

In some cases, the employees were required to purchase various software packages to perform the tasks required for their employment. The employees received a check and were instructed to keep a portion of the funds for supplies and wire the remaining funds to another individual. Once the employee wired the funds, the check was returned as counterfeit. The IC3 has received over 80 complaints identifying a twist to the scheme reporting that employees were asked to post employment advertisements on Craigslist and provide full details of a credit card, including owner name, address, card number, security code, and the expiration date of the card. In doing so, the victim unknowingly became a recruiter for the fraudster.

## NEW TWIST TO THE HIT MAN SCAM

Recent complaints reported to the IC3 identified a new twist to the Hit Man Scam The victims informed that the e-mails advised they have been targeted for assassination and asked them to purchase a security alarm to use if they see suspicious activity. The e-mails were signed by Agent Bauer of the International Intelligence Bureau and included the following language:

*You have been targeted for assassination over a past legal financial matters. A hired international assassin has been hired to kill you. All information and concrete evidence will be forwarded to you, but that should be after the apprehension of the assassin. Please do not disclose this information to any body, including any other enforcement personal in your region. Our effort to trap him might be jeopadise , if our strategies are expose by other enforcement agencies behind this crime. From this moment see anybody as somebody that wants to kill you.*

*The private international investigator tracking the assassin , wants you to purchase our device security alarm, as you are expected to press the device alarm if you suspect any activities . We can come to your rescue through any of our attached security personel, and this is possible within our network close to you in less than 10 minutes.*

*Please try to cooperate with us. We wait to hear from you.*

Recipients must be cautious of e-mails purportedly from any government agency endorsing a product or encouraging the recipient to send money for any reason. The United States government does not endorse products via e-mail.