INTERNET CRIME COMPLAINT CENTER'S (IC3)
SCAM ALERTS
NOVEMBER 26, 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.

TOP NINE FRAUD ATTACKS IMPACTING ECOMMERCE

A payment management company recently reported on the top fraud attacks most impactful to eCommerce. These attacks were identified by frequency of attack and revenue loss.

In ranked order, the top nine fraud attacks identified were:

9) Triangulation Schemes
8) Phishing/Pharming/Whaling
7) Botnets
6) Re-shipping
5) Affiliate Fraud
4) Identity Theft
3) Friendly Fraud
2) Account Takeover
1) Clean Fraud

FRAUD TARGETING DIRECT SALES COMPANIES

Several legitimate direct sales companies have seen a large surge in fake orders being places with their consultants. The consultants are contacted through the legitimate “find a consultant” link located on the various sales Websites. In each instance, the suspects are placing large orders and agreeing to pay by check. The consultant receives the check for a much larger amount than the total cost for the products. The consultants are instructed to cash the check and send the difference back to the buyer via wire transfer. The IC3 has received several complaints filed by consultants from companies affected by this scam.

For more information regarding online scams visit our Press Room page for the most current Public Service Announcements. https://www.ic3.gov/media/default.aspx