BUYER BEWARE

How To Avoid A Deal That's Not Real

(NAPS)—Millions of Americans shop online every day. Not only is it quick and convenient, but savvy Internet shoppers know that great deals are found on the Web.

But not every online offer is a genuine bargain. The Business Software Alliance (BSA) warns consumers to be wary of spam e-mail advertisements and Internet mail-order sites selling software at "bargain prices."

Although the software ads may look legitimate, this is often not the case. Bob Kruger, BSA's vice president of enforcement, cautions, "Spam 'deals' and mail-order sites seek to pass software off as genuine by using polished graphics and manufacturers' logos. Unfortunately, this is how software pirates dupe businesses and consumers into buying illegal software."

Why should businesses and consumers avoid pirated software? First, software piracy is illegal. Second, unlicensed software often functions improperly—if at all—or contains viruses. Last, the organizations selling fraudulent software may engage in other illicit behavior. Some consumers have complained of unapproved credit card charges, for example.

In an effort to protect businesses and consumers from the risks associated with pirated software, BSA and the Council of Better Business Bureaus offer the following tips:

1. **Don't Reply!** If you suspect an e-mail is spam, don't reply. Your address may be distributed to other spammers, thus increasing the volume of spam you receive. Indicators that an e-mail is spam include typos, misspellings and prices that are "too good to be true."

2. **Don't Post.** Avoid posting your e-mail address on public sites—spammers search public sites for e-mail addresses.

Not replying to spam is one of the best ways to avoid buying fraudulent software.

3. **Check Out the Dealer.** Review the software publisher's Web site. If the reseller isn't listed on the manufacturer's Web site as a recognized dealer, proceed with caution.

4. **Trust Your Instincts.** If a price seems "too good to be true," it probably is.

5. **Beware of Back-ups.** Take special care to avoid sellers offering "back-up" copies. This is an indication that the software is illegal.

6. **Do Your Homework.** Look for a feedback section on the site and look for comments about the seller based on previous transactions. Look for a trust mark from a reputable organization, like BBBOnLine, that signifies the merchant has agreed to a code of business practices.

7. **Get the Seller's Address.** Remember that if you cannot re-contact the seller, you may have no recourse if the product turns out to be pirated. If you can't find the seller's physical address, be suspicious.

8. **Keep Receipts.** Print out a copy of your order number and sales confirmation and keep them at least until your software arrives in satisfactory condition.

9. **Report Piracy.** Buyers suspecting software piracy, counterfeit software and/or fraud should contact law enforcement agencies and BSA at 1-888-NO PIRACY or www.bsa.org.