



# FEATURE STORY

## Bill Lockyer



### California Attorney General

### Protecting Consumers from Internet Fraud

Law enforcement can crack down on cyber thugs by keeping up-to-date on rapidly emerging Internet fraud schemes. Consumers can protect themselves from these cyber con artists by recognizing the danger signs of fraud, and taking steps to avoid it.

Last year, consumers filed more than 686,000 complaints with the Federal Trade Commission (FTC), with victims reporting losses of \$680 million. More than 93,000 Californians reported becoming victims, losing \$80 million. The top complaints were identity theft, bogus Internet auctions, foreign money offers, catalog sales and sweepstakes. Internet-related complaints accounted for 46 percent of all consumer fraud complaints.

#### Overpayment Scams

Recent ploys by con artists include convincing a seller to cash a money order worth more than the sale price of an item, then send the remainder to a third party for "shipping" or other purposes. In one recent case, thousands of dollars worth of counterfeit money orders were allegedly used to con people out of their funds. A person using the name "Susan Ford" created a fraudulent UPS account in an organization's name and began shipping packages and envelopes containing multiple money orders, often valued at \$950 each. The 45 recipients stated that they were advertising on-line for a roommate. Someone responded to their ad and sent them a money order as a deposit and the first month's rent, and then requested the balance to be sent to Nigeria for various purported reasons.

One victim from Sacramento lost \$3,500 in this scheme. He had placed a roommate advertisement online. An individual using the name Jessie Pink responded, forwarded pictures of herself, and wrote him that she was coming from Nigeria and that her uncle would send him a money order. She told him to take the amount he needed for the deposit and wire the remainder to a travel agent in Nigeria supposedly so that she could get an airline ticket to the United States. The victim did as he was told and sent the money. He was soon to learn the money order was counterfeit and that he had lost all his savings.

In another example, an online seller advertised an Alaskan Malamute dog for \$300, and the buyer offered an overdraft money order for \$1,000. The buyer requested that the remainder of the funds be sent to London to a company purportedly to handle shipping the dog. Similar activities have been observed in the sale of cars and other products.

Sellers should never accept funds for purposes other than the sale of the product they are offering. The purposeful overpayment on a product should be a warning sign that the money order or other financial instrument is no good.

#### Online Auctions

Even buying the product itself can be problematic if the buyer relies on deceptive Internet auctions. The FTC reports a growing number of complaints about late shipments, no shipments, shipments of products of lesser quality than advertised, and bogus online payment services.

In one case investigated by the FTC, consumers allegedly "won" an Internet auction for computer software and electronics, sent in their money, but never received their merchandise. Two defendants allegedly continued to change their auction account names to conceal the fact that they never delivered promised merchandise.

Many online auctions list items that people want to sell, but do not verify the condition of the merchandise and cannot guarantee that sellers will keep their promises. Buyers should contact state or local consumer protection agencies and the Better Business Bureau to check the reputation of the auction site before using it.

Also, buyers should watch for the use of "shills," a practice whereby a seller may try to raise the price artificially by making bids under fictitious names. Using bogus bidders is illegal and a violation of online auction policies.



Buyers should be careful if the seller is a private individual, because many consumer protection laws do not apply to private sales, although government agencies may take action if criminal fraud is involved. When sellers from other countries are involved, extra precautions should be taken. The distance and difference in legal systems could make resolving a conflict difficult.

Consumers should obtain the seller's name, physical street address, e-mail address and phone number, and refuse to do business with anyone who does not provide this information.

Those who decide to purchase a product online should use a credit card. Under federal law, individuals can dispute charges if they paid the seller with a credit card and the goods were never delivered.

Understanding how Internet auctions work can help avoid problems. The FTC provides valuable information in "Internet Auctions: A Guide for Buyers and Seller" at [www.ftc.gov/bcp/conline/pubs/online/auctions.htm](http://www.ftc.gov/bcp/conline/pubs/online/auctions.htm).

### **Prizes and Sweepstakes**

Consumers should avoid falling victim to techniques that scammers use to con an unsuspecting individual who has "won a prize." Consumers should never "pay to play." It is illegal for a company to require anyone to buy something or pay a fee in order to win or claim a prize. Individuals should be wary of requests to send an "advance" on "winnings." It is illegal for a company to suggest that someone's chances will be better if he or she makes a purchase. Another trick to solicit money illegally is to claim that taxes must be paid on the prize before receiving it. It is up to the consumer to declare the prize winnings when filing income taxes.

It is important never to give credit card, bank account, or Social Security numbers to win a sweepstakes. No legitimate sweepstakes company asks for this information.

### **"Phishing"**

One of the most common measures used by sophisticated identity thieves are official-looking e-mails to trick consumers to "update" or "validate" their information, including their account number, Social Security number, or password. This is called "phishing." Sometimes the con artist will say that the potential victim's account is about to be closed, or an order for something has been placed in his name, or his

information has been lost because of a computer problem, or that fraud has occurred against his account.

This spam (unsolicited mail) often uses legitimate-sounding names of companies -- using all or part of a company's name -- and includes a link that closely resembles its web site, complete with company logo and color schemes. Small and large companies have been "spoofed" in this way to trick consumers into disclosing confidential information.

It is a felony in California to use the personal identifying information of another person without the authorization of that person for any unlawful purpose including to obtain credit, goods, services, or medical information [Penal Code section 530.5 et. seq.]. California also requires businesses and government agencies to notify consumers if hackers gain entry to computers that contain unencrypted personal information such as credit card numbers, pass codes needed for use of personal accounts, Social Security numbers, or driver's license numbers. Under state law (AB 1386-Peace/CHAPTER 915, Stats of 2002.), notices must be given immediately following discovery of the privacy breach unless a law enforcement agency determines the notice would impede a criminal investigation. Any customer injured by a violation of the law may file a civil suit to recover damages.

To avoid e-mail scams, consumers should be wary if they receive mail that contains generic greetings, such as "Dear AT&T Member," or a false sense of urgency. They should not open the mail, but delete it. If opened, it could expose their computer to viruses or devices that can record everything typed, including user passwords and account information, and have the data sent automatically to the identity thief or be harvested later.

### **Computer Protection**

Additionally, to help avoid Internet fraud, Californians should protect their computers from being exposed to misuse by con artists. Consumers should install anti-virus software to protect their computer from viruses, worms, trojan horses, adware and spyware. This software should be updated frequently and kept on. It should include a firewall, which blocks invasive attacks.

Individuals should update their computer's operating system, browser and other programs on a regular basis by downloading the most current "patches," which fix bugs, add new features and close security "holes" that can allow infections into a computer.

Continued on Page 16



Continued from Page 15

When purchasing products online, computer users should be sure to use a secure site. The https://, instead of the http://, sign at the top of screen, which includes an "s," means that the site is secure. The unbroken key symbol or locked padlock icon at the bottom of the screen also means that private information, such as a credit card number, is more likely to be secure when transmitted electronically to the company.

Login access codes (user name and password) should not be shared with anyone, and passwords should be changed on a regular basis.

Computer users should always "logout" of online sessions that require a password or login process, and close out the browser. Unauthorized transactions and activity can occur if online sessions are accessible to other people.

They should also check bills and credit reports frequently to be sure that no one is using their accounts. Free credit reports can be ordered through [www.annualcreditreport.com](http://www.annualcreditreport.com) or by calling (877) 322-8228.

For law enforcement, the Department of Justice offers "Computer/Internet Crime Investigations," a 32-hour course designed to provide investigators with the necessary training, skills, knowledge, and practical experience to conduct a variety of on-line crime investigations on emerging cyber crimes. For information on this course, please contact the Advanced Training Center at (916) 464-1200.

Additional information for consumers on protecting themselves against fraud is available on the Internet at:

- [www.onguardonline.gov](http://www.onguardonline.gov)
- <http://ag.ca.gov/consumers/alert.htm>
- [www.ftc.gov](http://www.ftc.gov), [www.usdoj.gov/criminal/fraud/idtheft.html](http://www.usdoj.gov/criminal/fraud/idtheft.html)
- [www.fraud.org](http://www.fraud.org).

Anyone who believes that he or she has been scammed should file a report with local law enforcement and a complaint at [www.ftc.gov](http://www.ftc.gov) or at the Internet Crime Complaint Center at [www.ic3.gov](http://www.ic3.gov).



**American Homeland Solutions**  
Homeland Security And Public Safety Services

**"ODP" Certified NIMS & SEMS Training**

*American Homeland Solutions* specializes in homeland security and public safety consulting services including management reviews; emergency response preparedness training, evaluation and exercises; terrorism and vulnerability assessments; infrastructure protection evaluations; background and personnel investigations; and other services tailored to the clients' needs.

**AHS**  
American Homeland Solutions

**WILLDAN** | **MuniFinancial** | **ARROYO**  
Serving Public Agencies | GEOTECHNICAL

Engineering, Planning, Financial and Economic Consulting, and Geotechnical Engineering.

American Homeland Solutions: 714/940-6370 [www.americanhomelandsolutions.com](http://www.americanhomelandsolutions.com)  
Willdan: 800/424-9144 [www.willdan.com](http://www.willdan.com) | MuniFinancial: 800/755-MUNI (6864) [www.muni.com](http://www.muni.com)  
Arroyo Geotechnical: 714/634-3318 [www.arroyogeotechnical.com](http://www.arroyogeotechnical.com)