DEPARTMENT OF
CORPORATIONS
State of California • Business, Transportation and Housing Agency

ONLINE ESCROW FRAUD
Questions & Answers

Q. **What is an online escrow company?**

A. Online escrow companies are used to pay for items found through online auction sites and marketplaces that advertise classified ads, usually for expensive items like computers, electronics, cars, and jewelry. Some Internet auction sites, like eBay, recommend that their users pay for purchases over $500 through an online escrow company.

Escrow providers help prevent fraud by acting as independent third parties between buyers and sellers. After the escrow company receives the buyer's check, money order or credit card payment, the company notifies the seller to ship the purchase to the buyer. The escrow company does not forward the buyer's payment to the seller until the buyer receives the item. Buyers usually pay the escrow service fees, which are generally a percentage of the purchased item's cost.

Q. **How are online escrow companies licensed and regulated in California?**

A. Persons or companies performing escrow services over the Internet in California, or performing escrow services for consumers in California, must comply with the licensing requirements of the California Escrow Law. The licensing and regulatory process ensures that companies' owners and key employees have been subject to background checks performed by the California Department of Corporations, that the company's financial condition and records are adequate, that the company is properly bonded, and that all customer funds are segregated in trust fund accounts until the terms of the escrow are met.

Q. **How many escrow companies are licensed by the Department of Corporations?**

A. There are about 650 independent escrow companies in California licensed by the Department of Corporations. The Department licenses only one **online** escrow service: www.escrow.com.

Q. **How are fraudulent online escrow Web sites set up?**

A. Stolen identities and credit card numbers are used to open a Web hosting account, and the scammers upload content files to the Web hosting server to create a fake escrow service Web site. Sometimes a phony escrow company site can be detected by its sloppy content, with spelling and grammar errors and inconsistent information. Other times, the site's information may have been copied from legitimate escrow company Web sites.

Fraudulent escrow company sites often claim to be licensed by the California Department of Corporations and may provide a link to the Department's Web site. The sites use a phony license number or use one of the Department's current licensee's license number and address.

Fake escrow company sites often display logos from the Better Business Bureau, VeriSign Secure, TRUSTe, and even the Internet Fraud Complaint Center.

When fraudulent escrow company sites are detected and shut down, the scammers copy the defunct site's files and create a new site, changing little more than the domain name, and are quickly back in business.

Q. **How are consumers victimized by fake online escrow companies?**

A. The scammers trick online auction or classified ad buyers by setting up phony auctions or posting fake ads. The "seller" tells the interested buyer to use a particular online escrow company to complete the transaction. The buyer sends the payment to the phony escrow services site, but never receives the promised merchandise in return.

Sellers can be victims, too. The scammer may pose as a "buyer" or the winning bidder in an online auction and tells the seller to use a particular online escrow company. The seller receives an e-mail from the fraudulent escrow company indicating the buyer has sent the payment to the escrow company. The seller ships the merchandise to the address provided by the scam artist – often a hotel lobby or mailbox rental store – but never receives payment.

Q. **Who is committing these online escrow scams?**

A. According to the Internet Crime Complaint Center, many of these frauds originate in Eastern Europe in former communist countries.

Q. **What other methods do fraudulent escrow company site operators use to avoid detection?**

Sometimes scammers set up a third party to receive funds or merchandise.

The fraudster sends an e-mail to an unsuspecting job seeker who has posted a resume on HotJobs, Monster, or a similar site. The e-mail may indicate the job seeker is perfect for a "National Accounts Manager" position acting on behalf of a group of "independent distributors, well-known in Europe selling electronics," who want to enter the U.S. market. The job seekers use their bank account to receive funds and wire proceeds from the "large equipment sales" to the "company headquarters" overseas, usually in Latvia, Estonia, Romania, or Cyprus. The job seeker then keeps 8% of the transferred funds as his commission.

Other job seekers are recruited and paid to forward merchandise to con artists. This job seeker, hired as a middleman, forwards the package overseas. The scammed seller receives nothing for the merchandise.

Q. **How widespread is fraudulent online escrow activity?**

A. The Department has taken enforcement actions against 33 Internet escrow providers to shut down fraudulent escrow sites since May 2004. None of these online escrow companies applied for licenses to operate legitimately in California.
There are hundreds of unlicensed and/or fraudulent online escrow Web sites.

Q. **How much money is lost in California due to fraudulent online escrow activity?**

A. The amount is difficult to track but is believed to be significant given the amount of potential activity on these sites. The Escrow Fraud Task Force should be able to assess the monetary loss.

Q. **How can California consumers protect themselves against online escrow fraud?**

A. Californians can call the California Department of Corporations toll-free at **1-866-ASK-CORP (1-866-275- 2677)** to make sure the escrow company you plan to use is properly licensed.

Here are more tips for online shoppers to avoid escrow fraud.

- Never disclose financial or personal information like your Social Security number, credit card number, or bank account information until you have verified that the online escrow company you are using is properly licensed.

- A buyer or seller who insists on using a particular escrow company is probably trying to steer you towards a fraudulent escrow services site.

- Watch out for escrow company sites that don't have an address and phone number listed. If the site does list a phone number, call the number and be sure you speak to a live person. A generic voice mail is a sign that the company may be fraudulent.

- Send the escrow company an e-mail question. If you don't receive a response, don't do business with them.

- Sometimes a phony escrow company Web site can be detected by its sloppy content, with spelling and grammar errors and inconsistent information. Other times, the site's information may have been copied from legitimate escrow company sites.

- Find out how the online escrow service processes transactions. Steer clear of sites that don't process their own, but require users to set up accounts with online payment services instead. Legitimate escrow companies don't use person-to-person money transfers like Western Union or MoneyGram or direct you to send your payment to an individual rather than a corporate entity.

- Fake escrow company sites often display logos from the Better Business Bureau, VeriSign Secure, TRUSTe, and even the Internet Fraud Complaint Center. Check to make sure the escrow company really is endorsed by these organizations.

- Avoid escrow company sites with domain names ending in .org, .biz, .cc, .info., or .US.

- Be wary of a seemingly terrific deal. Scammers post online classified ads and offer items via online auction with very low prices. Remember, these so-called "deals" are just the hook to get you to use a phony escrow company site.

Q. **What can California consumers do if they think they've been taken by an online escrow scam?**

A. If you think you've fallen victim to an online escrow scam, you should file a complaint with the California Department of Corporations. Complaint forms can be found at **www.corp.ca.gov**, or call **1-866-ASK-CORP (1-866-275-2677)** to have a complaint form sent to you.

You should also file a complaint with the Internet Crime Complaint Center (IC3) by going to **http://www.ic3.gov**. The IC3 is a partnership between the FBI and the National White Collar Crime Center created to address fraud committed over the Internet.

If you've given personal information such as your bank account or credit card number to a fraudulent Internet escrow company, you need to take steps to resolve potential identity theft-related problems. The California Department of Consumer Affairs' Office of Privacy Protection offers information about what to do if you believe you may be a victim of identity theft: **http://www.privacy.ca.gov/cover/identitytheft.htm**.

12/04