

Internet Fraud

Sandra A. Smith

"Internet auction fraud was by far the most reported offense, comprising 44.9% of referred complaints. Non-delivered merchandise and/or payment accounted for 19.0% of complaints. Check fraud made up 4.9% of complaints. Credit/debit card fraud, computer fraud, confidence fraud, and financial institutions fraud round out the top seven categories of complaints referred to law enforcement during the year."

Listed below are tips to protect yourself and your family from various forms of Internet fraud:

Avoiding Internet Auction Fraud

* Understand as much as possible about how the auction works, what your obligations are as a buyer, and what the seller's obligations are before you bid.

* Find out what actions the web site/company takes if a problem occurs and consider insuring the transaction and shipment.

* Learn as much as possible about the seller, especially if the only information you have is an e-mail address. If it is a business, check the Better Business Bureau where the seller/business is located.

* Examine the feedback on the seller.

* Determine what method of payment the seller is asking from the buyer and where he/she is asking to send payment.

* If a problem occurs with the auction transaction, it could be much more difficult if the seller is located outside the US because of the difference in laws.

* Ask the seller about when delivery can be expected and if there is a problem with the merchandise is it covered by a warranty or can you exchange it.

* Find out if shipping and delivery are included in the auction price or are additional costs so there are no unexpected costs.

* There should be no reason to give out your social security number or drivers license number to the seller.

Avoiding Non-Delivery of Merchandise

* Make sure you are purchasing merchandise from a reputable source.

* Do your homework on the individual or company to ensure that they are legitimate.

* Try to obtain a physical address rather than merely a post office box and a phone number, call the seller to see if the number is correct and working.

* Send them e-mail to see if they have an active e-mail address and be wary of sellers who use free e-mail services where a credit card wasn't required to open the account.

* Consider not purchasing from sellers who won't provide you with this type of information.

* Check with the Better Business Bureau from the seller's area.

* Check out other web sites regarding this person/company.

* Don't judge a person/company by their web site.

* Be cautious when responding to special offers (especially through unsolicited e-mail).

* Be cautious when dealing with individuals/companies from outside your own country.

* Inquire about returns and warranties.

* The safest way to purchase items via the Internet is by credit card because you can often dispute the charges if something is wrong.

* Make sure the transaction is secure when you electronically send your credit card numbers.

* Consider utilizing an escrow or alternate payment service.

Avoiding Credit Card Fraud

* Don't give out your credit card number(s) online unless the site is a secure and reputable site. Sometimes a tiny icon of a padlock appears to symbolize a higher level of security to transmit data. This icon is not a guarantee of a secure site, but might provide you some assurance.

* Don't trust a site just because it claims to be secure.

* Before using the site, check out the security/encryption software it uses.

* Make sure you are purchasing merchandise from a reputable source.

* Do your homework on the individual or company to ensure that they are legitimate.

* Try to obtain a physical address rather than merely a post office box and a phone number, call the seller to see if the number is correct and working.

* Send them e-mail to see if they have an active e-mail address and be wary of sellers who use free e-mail services

where a credit card wasn't required to open the account.

* Consider not purchasing from sellers who won't provide you with this type of information.

* Check with the Better Business Bureau from the seller's area.

* Check out other web sites regarding this person/company.

* Don't judge a person/company by their web site.

* Be cautious when responding to special offers (especially through unsolicited e-mail).

* Be cautious when dealing with individuals/companies from outside your own country.

* The safest way to purchase items via the Internet is by credit card because you can often dispute the charges if something is wrong.

* Make sure the transaction is secure when you electronically send your credit card numbers.

* You should also keep a list of all your credit cards and account information along with the card issuer's contact information. If anything looks suspicious or you lose your credit card(s) you should contact the card issuer immediately.

Avoiding Investment Fraud

* Don't invest in anything based on appearances. Just because an individual or company has a flashy web site doesn't mean it is legitimate. Web sites can be created in just a few days. After a short period of taking money, a site can vanish without a trace.

* Don't invest in anything you are not absolutely sure about. Do your homework on the investment to ensure that it is legitimate.

* Do your homework on the individual or company to ensure that they are legitimate.

* Check out other web sites regarding this person/company.

* Don't judge a person/company by their web site.

* Be cautious when responding to special investment offers (especially through unsolicited e-mail).

* Be cautious when dealing with individuals/companies from outside your own country.

* Inquire about all the terms and conditions.

* If it sounds too good to be true it probably is.

Avoiding Business Fraud

* Purchase merchandise from reputable dealers or establishments.

* Try to obtain a physical address rather than merely a post office box and a phone number, call the seller to see if the number is correct and working.

* Send them e-mail to see if they have an active e-mail address and be wary of those that utilize free e-mail services where a credit card wasn't required to open the account.

* Consider not purchasing from sellers who won't provide you with this type of information.

* Purchase merchandise directly from the individual/company that holds the trademark, copyright, or patent.

* Beware when responding to e-mail that may not have

been sent by a reputable company.

Avoiding the Nigerian Letter Scam

* Be skeptical of individuals representing themselves as Nigerian or foreign government officials asking for your help in placing large sums of money in overseas bank accounts.

* Do not believe the promise of large sums of money for your cooperation.

* Guard your account information carefully.

Telemarketing Fraud

When you send money to people you do not know personally or give personal or financial information to unknown callers, you increase your chances of becoming a victim of telemarketing fraud.

Warning signs -- what a caller may tell you:

- "You must act 'now' or the offer won't be good."

- "You've won a 'free' gift, vacation, or prize." But you have to pay for "postage and handling" or other charges.

- "You must send money, give a credit card or bank account number, or have a check picked up by courier." You may hear this before you have had a chance to consider the offer carefully.

- "You don't need to check out the company with anyone." The callers say you do not need to speak to anyone including your family, lawyer, accountant, local Better Business Bureau, or consumer protection agency.

- "You don't need any written information about their company or their references."

- "You can't afford to miss this 'high-profit, no-risk' offer."

If you hear these--or similar--"lines" from a telephone salesperson, just say "no thank you," and hang up the phone.

Some Tips to Avoid Telemarketing Fraud:

It's very difficult to get your money back if you've been cheated over the phone. Before you buy anything by telephone, remember:

* Don't buy from an unfamiliar company. Legitimate businesses understand that you want more information about their company and are happy to comply.

* Always ask for and wait until you receive written material about any offer or charity. If you get brochures about costly investments, ask someone whose financial advice you trust to review them. But, unfortunately, beware -- not everything written down is true.

* Always check out unfamiliar companies with your local consumer protection agency, Better Business Bureau, state Attorney General, the National Fraud Information Center, or other watchdog groups. Unfortunately, not all bad businesses can be identified through these organizations.

* Obtain a salesperson's name, business identity, telephone number, street address, mailing address, and business license number before you transact business. Some con artists give out false names, telephone numbers, addresses, and business license numbers. Verify the accuracy of these items.

* Before you give money to a charity or make an investment, find out what percentage of the money is paid in com-

missions and what percentage actually goes to the charity or investment.

* Before you send money, ask yourself a simple question. "What guarantee do I really have that this solicitor will use my money in the manner we agreed upon?"

* You must not be asked to pay in advance for services. Pay services only after they are delivered.

* Some con artists will send a messenger to your home to pick up money, claiming it is part of their service to you. In reality, they are taking your money without leaving any trace of who they are or where they can be reached.

* Always take your time making a decision. Legitimate companies won't pressure you to make a snap decision.

* Don't pay for a "free prize." If a caller tells you the payment is for taxes, he or she is violating federal law.

* Before you receive your next sales pitch, decide what your limits are -- the kinds of financial information you will and won't give out on the telephone.

* It's never rude to wait and think about an offer. Be sure to talk over big investments offered by telephone salespeople with a trusted friend, family member, or financial advisor.

* Never respond to an offer you don't understand thoroughly.

* Never send money or give out personal information such as credit card numbers and expiration dates, bank account numbers, dates of birth, or social security numbers to unfamiliar companies or unknown persons.

* Your personal information is often brokered to telemarketers through third parties.

* If you have information about a fraud report it to state, local, or federal law enforcement agencies.

Nigerian Letter or "419" Fraud

Nigerian letter frauds combine the threat of impersonation fraud with a variation of an advance fee scheme in which a letter, mailed from Nigeria, offers the recipient the "opportunity" to share in a percentage of millions of dollars that the author, a self-proclaimed government official, is trying to transfer illegally out of Nigeria. The recipient is encouraged to send information to the author, such as blank letterhead stationery, bank name and account numbers and other identifying information using a facsimile number provided in the letter. Some of these letters have also been received via E-mail through the Internet. The scheme relies on convincing a willing victim, who has demonstrated a "propensity for larceny" by responding to the invitation, to send money to the author of the letter in Nigeria in several installments of increasing amounts for a variety of reasons.

Payment of taxes, bribes to government officials, and legal fees are often described in great detail with the promise that all expenses will be reimbursed as soon as the funds are spirited out of Nigeria. In actuality, the millions of dollars do not exist and the victim eventually ends up with nothing but loss. Once the victim stops sending money, the perpetrators have been known to use the personal information and checks that they received to impersonate the victim, draining bank accounts and credit card balances until the victim's assets are taken in their entirety. While such an invitation impresses most law-abiding citizens as a laughable hoax, millions of

dollars in losses are caused by these schemes annually. Some victims have been lured to Nigeria, where they have been imprisoned against their will, in addition to losing large sums of money. The Nigerian government is not sympathetic to victims of these schemes, since the victim actually conspires to remove funds from Nigeria in a manner that is contrary to Nigerian law. The schemes themselves violate section 419 of the Nigerian criminal code, hence the label "419 fraud."

Some Tips to Avoid Nigerian Letter or "419" Fraud:

* If you receive a letter from Nigeria asking you to send personal or banking information, do not reply in any manner. Send the letter to the U.S. Secret Service or the FBI.

* If you know someone who is corresponding in one of these schemes, encourage that person to contact the FBI or the U.S. Secret Service as soon as possible.

* Be skeptical of individuals representing themselves as Nigerian or foreign government officials asking for your help in placing large sums of money in overseas bank accounts.

* Do not believe the promise of large sums of money for your cooperation.

* Guard your account information carefully.

Impersonation/Identity Fraud

Impersonation fraud occurs when someone assumes your identity to perform a fraud or other criminal act. Criminals can get the information they need to assume your identity from a variety of sources, such as the theft of your wallet, your trash, or from credit or bank information. They may approach you in person, by telephone, or on the Internet and ask you for the information.

The sources of information about you are so numerous that you cannot prevent the theft of your identity. But you can minimize your risk of loss by following a few simple hints.

Some Tips to Avoid Impersonation/Identity Fraud:

* Never throw away ATM receipts, credit statements, credit cards, or bank statements in a usable form.

* Never give your credit card number over the telephone unless you make the call.

* Reconcile your bank account monthly and notify your bank of discrepancies immediately.

* Keep a list of telephone numbers to call to report the loss or theft of your wallet, credit cards, etc.

* Report unauthorized financial transactions to your bank, credit card company, and the police as soon as you detect them.

* Review a copy of your credit report at least once each year. Notify the credit bureau in writing of any questionable entries and follow through until they are explained or removed.

* If your identity has been assumed, ask the credit bureau to print a statement to that effect in your credit report.

* If you know of anyone who receives mail from credit card companies or banks in the names of others, report it to local or federal law enforcement authorities.

Advance Fee Scheme

An advance fee scheme occurs when the victim pays money to someone in anticipation of receiving something of greater value, such as a loan, contract, investment, or gift, and then receives little or nothing in return.

The variety of advance fee schemes is limited only by the imagination of the con artists who offer them. They may involve the sale of products or services, the offering of investments, lottery winnings, "found money," or many other "opportunities." Clever con artists will offer to find financing arrangements for their clients who pay a "finder's fee" in advance. They require their clients to sign contracts in which they agree to pay the fee when they are introduced to the financing source. Victims often learn that they are ineligible for financing only after they have paid the "finder" according to the contract. Such agreements may be legal unless it can be shown that the "finder" never had the intention or the ability to provide financing for the victims.

Some Tips to Avoid the Advanced Fee Schemes:

* If the offer of an "opportunity" appears too good to be true, it probably is. Follow common business practice. For example, legitimate business is rarely conducted in cash on a street corner.

* Know who you are dealing with. If you have not heard of a person or company that you intend to do business with, learn more about them. Depending on the amount of money that you intend to spend, you may want to visit the business location, check with the Better Business Bureau, or consult with your bank, an attorney, or the police.

* Make sure you fully understand any business agreement that you enter into. If the terms are complex, have them reviewed by a competent attorney.

* Be wary of businesses that operate out of post office boxes or mail drops and do not have a street address, or of dealing with persons who do not have a direct telephone line, who are never "in" when you call, but always return your call later.

* Be wary of business deals that require you to sign non-disclosure or noncircumvention agreements that are designed to prevent you from independently verifying the bona fides of the people with whom you intend to do business. Con artists often use noncircumvention agreements to threaten their victims with civil suit if they report their losses to law enforcement.

Common Health Insurance Frauds

Medical Equipment Fraud:

Equipment manufacturers offer "free" products to individuals. Insurers are then charged for products that were not needed and/or may not have been delivered.

"Rolling Lab" Schemes:

Unnecessary and sometimes fake tests are given to indi-

viduals at health clubs, retirement homes, or shopping malls and billed to insurance companies or Medicare.

Services Not Performed:

Customers or providers bill insurers for services never rendered by changing bills or submitting fake ones.

Medicare Fraud:

Medicare fraud can take the form of any of the health insurance frauds described above. Senior citizens are frequent targets of Medicare schemes, especially by medical equipment manufacturers who offer seniors free medical products in exchange for their Medicare numbers. Because a physician has to sign a form certifying that equipment or testing is needed before Medicare pays for it, con artists fake signatures or bribe corrupt doctors to sign the forms. Once a signature is in place, the manufacturers bill Medicare for merchandise or service that was not needed or was not ordered.

Some Tips to Avoid the Health Insurance Fraud:

* Never sign blank insurance claim forms.

* Never give blanket authorization to a medical provider to bill for services rendered.

* Ask your medical providers what they will charge and what you will be expected to pay out-of-pocket.

* Carefully review your insurer's explanation of the benefits statement. Call your insurer and provider if you have questions.

* Do not do business with door-to-door or telephone salespeople who tell you that services of medical equipment are free.

* Give your insurance/Medicare identification only to those who have provided you with medical services.

* Keep accurate records of all health care appointments.

* Know if your physician ordered equipment for you.

Investment Related Scams:

Letter of Credit Fraud

Legitimate letters of credit are never sold or offered as investments.

Legitimate letters of credit are issued by banks to ensure payment for goods shipped in connection with international trade. Payment on a letter of credit generally requires that the paying bank receive documentation certifying that the goods ordered have been shipped and are en route to their intended destination.

Letters of credit frauds are often attempted against banks by providing false documentation to show that goods were shipped when, in fact, no goods or inferior goods were shipped.

Other letter of credit frauds occur when con artists offer a "letter of credit" or "bank guarantee" as an investment wherein the investor is promised huge interest rates on the order of 100 to 300 percent annually. Such investment "opportunities" simply do not exist. (See Prime Bank Notes for

additional information.)

Some Tips to Avoid Letter of Credit Fraud:

* If an "opportunity" appears too good to be true, it probably is.

* Do not invest in anything unless you understand the deal. Con artists rely on complex transactions and faulty logic to "explain" fraudulent investment schemes.

* Do not invest or attempt to "purchase" a "Letter of Credit." Such investments simply do not exist.

* Be wary of any investment that offers the promise of extremely high yields.

* Independently verify the terms of any investment that you intend to make, including the parties involved and the nature of the investment.

Prime Bank Note

International fraud artists have invented an investment scheme that offers extremely high yields in a relatively short period of time. In this scheme, they purport to have access to "bank guarantees" which they can buy at a discount and sell at a premium. By reselling the "bank guarantees" several times, they claim to be able to produce exceptional returns on investment. For example, if \$10 million worth of "bank guarantees" can be sold at a two percent profit on ten separate occasions, or "tranches," the seller would receive a 20 percent profit. Such a scheme is often referred to as a "roll program." To make their schemes more enticing, con artists often refer to the "guarantees" as being issued by the world's "Prime Banks," hence the term "Prime Bank Guarantees." Other official sounding terms are also used such as "Prime Bank Notes" and "Prime Bank Debentures." Legal documents associated with such schemes often require the victim to enter into non-disclosure and noncircumvention agreements, offer returns on investment in "a year and a day", and claim to use forms required by the International Chamber of Commerce (ICC). In fact, the ICC has issued a warning to all potential investors that no such investments exist.

The purpose of these frauds is generally to encourage the victim to send money to a foreign bank where it is eventually transferred to an off-shore account that is in the control of the con artist. From there, the victim's money is used for the perpetrator's personal expenses or is laundered in an effort to make it disappear.

While foreign banks use instruments called "bank guarantees" in the same manner that U.S. banks use letters of credit to insure payment for goods in international trade, such bank guarantees are never traded or sold on any kind of market.

Some Tips to Avoid Prime Bank Note Related Fraud:

* Think before you invest in anything. Be wary of an investment in any scheme, referred to as a "roll program," that offers unusually high yields by buying and selling anything issued by "Prime Banks."

* As with any investment perform due diligence. Independently verify the identity of the people involved, the verac-

ity of the deal, and the existence of the security in which you plan to invest.

* Be wary of business deals that require nondisclosure or noncircumvention agreements that are designed to prevent you from independently verifying information about the investment.

What is a "Ponzi" Scheme?

A Ponzi scheme is essentially an investment fraud wherein the operator promises high financial returns or dividends that are not available through traditional investments. Instead of investing victims' funds, the operator pays "dividends" to initial investors using the principle amounts "invested" by subsequent investors. The scheme generally falls apart when the operator flees with all of the proceeds, or when a sufficient number of new investors cannot be found to allow the continued payment of "dividends."

This type of scheme is named after Charles Ponzi of Boston, Massachusetts, who operated an extremely attractive investment scheme in which he guaranteed investors a 50 percent return on their investment in postal coupons. Although he was able to pay his initial investors, the scheme dissolved when he was unable to pay investors who entered the scheme later.

Some Tips to Avoid Ponzi Schemes:

* As with all investments, exercise due diligence in selecting investments and the people with whom you invest.

* Make sure you fully understand the investment before you invest your money.

Pyramid Scheme

Pyramid schemes, also referred to as franchise fraud, or chain referral schemes, are marketing and investment frauds in which an individual is offered a distributorship or franchise to market a particular product. The real profit is earned, not by the sale of the product, but by the sale of new distributorships. Emphasis on selling franchises rather than the product eventually leads to a point where the supply of potential investors is exhausted and the pyramid collapses. At the heart of each pyramid scheme there is typically a representation that new participants can recoup their original investments by inducing two or more prospects to make the same investment. Promoters fail to tell prospective participants that this is mathematically impossible for everyone to do, since some participants drop out, while others recoup their original investments and then drop out.

Some Tips to Avoid Pyramid Schemes:

* Be wary of "opportunities" to invest your money in franchises or investments that require you to bring in subsequent investors to increase your profit or recoup your initial investment.

* Independently verify the legitimacy of any franchise or investment before you invest. Nov 05-08, 2007 2007 | QC | Montreal

Journal of Medical Sciences Research (JMSR)

<http://jmsr.org/>

is an independent, international general medical journal
supporting academic freedom and open access.
