# Dealing with Financial Fraud

*Last update: February 5, 2013*


## Summary

Everyone is potentially vulnerable to financial scams, but older people often are deliberate targets of con artists. This paper helps you watch out for signs that someone is trying to take advantage of you, and advises you how to react at the time, and what to do if you find out that you have already been cheated.


## The spectrum of fraud: from overpricing to identity theft

For our purposes, fraud includes any financial transaction in which you would not participate if you had all the facts. This is a looser definition than the legal one. If a salesperson talks you into, say, a home improvement that you don't really need, or that costs twice what you might pay elsewhere, that is not illegal. But you are being taken advantage of all the same, and the consequences are not all that different from outright theft.

Other offers are outright scams: the product or service does not even exist. You are asked to pay up front, or to provide a bank account or credit card number, or other forms of assets or documents or information that will be used to your financial disadvantage.

Increasingly, "identity theft" is becoming an issue. This might be as simple as someone using your credit card or credit account information to make purchases. Or someone might use your Social Security Number to open new accounts or engage in other transactions that can cause you financial losses, ruin your credit rating, and lead to bureaucratic nightmares for you as you try to straighten it all out.

There are many kinds of scams, too many to describe separately here, and new ones are constantly being invented. So we will focus mainly on general tips for preventing, identifying, and coping with fraud. (Individual kinds of scams are described in some of the web sites we refer to at the end of this paper.)

## Preventing fraud

The most important general rules are:

- "If it sounds too good to be true, it is." We've all heard that, and it's true – yet we also hope that *this* time a hot tip or a cozy deal will pay off. Yes, there's a chance of that, but if you can't afford to lose your money, don't gamble. Odds are that a great-sounding deal is either a long-shot risk or a flat-out fraud.
- Don't trust people you don't know with your money or your personal information, no matter how nice and sincere the people seem. Almost all successful scammers are nice and sincere. Be friendly to strangers if you want to be, but pull back if they ask you for money or personal data.
- Con artists will say *anything*: that they are contacting you about someone else having victimized you, or even that a loved one has been in an accident or for some other reason needs money urgently. We tend to suspend our normal judg-

ment in emergencies, but instead you should be extra careful. If someone wants your money, no matter what the reason, and itôs not someone you know, donôt give it to them until you can verify their story and their credentials.

- Check out anyone who claims to be a financial advisor, even if she or he has impressive credentials, if an offer sounds suspiciously good. (See the notes at the end of this paper for ways to do this.)
- If you do need to provide money or information (credit card info, Social Security Number, bank account number, tax records, etc.), be *certain* you know whom you are dealing with. If someone contacted you first, assume that any identification they gave you is fraudulent until proven otherwise. Offer to get back to them after you check them out ï and then do check them out, using a telephone number from a public phone listing, not a number the person gave you.
- Get any offer in writing. If you canôt get it in writing, walk away.
- Be doubly suspicious of any offer that requires you to send money by wire or courier, or to send money to a foreign country. These techniques are used to make it hard to get your money back, and for authorities to intervene.
- Never agree to any offer for a product or service, and especially a financial product or service, until you are sure you understand it completely, including the small print. If itôs so complicated that it doesnôt make sense to you, just say no.
- For any important financial commitment, sleep on it. If the offer wonôt wait, it is most likely a scam. If you have any doubts at all, get a second opinion from a trusted family member, friend, or paid advisor.
- Review your credit card statements for unauthorized transactions. Keep receipts and statements, so you can verify past transactions if you need to.
- If you feel unsure about your vulnerability, have a trusted family member review financial statements and decisions for you. Even if you feel comfortable with your own financial knowledge, a second pair of eyes can help spot problems.

More specifically:

<u>On the telephone</u>:

- Scammers often target retired people on the telephone, because retirees often have cash at their disposal, but also because they generally have time to chat, and often feel lonely or bored and eager to talk, even to strangers. Then, once a connection and some trust has been established, the scam comes out, and it always sounds so, so plausible. The more a stranger acts friendly to you, the more suspicious you should be. As soon as the discussion veers toward money, or credit cards, or any related subject, get off the phone (graciously or not, as you prefer!).
- If you find it hard to hang up on people, use an answering machine to screen calls.
- Just because someone *says* they are from your bank or credit card company, or from your church or club or company, this doesnôt mean they really are. Before

you give any personal or financial information to such a person, and certainly before you give them any money, verify the connection independently.

- *Unless <u>you</u> made the phone call*, never give your credit card number, Social Security Number, or other personal identifying information over the phone to someone you otherwise don't know.

<u>On the computer</u>:

- Never respond to spam email in *any* way, other than deleting it, and never open attachments to emails unless they came from someone you know and unless you already have a good idea what's in them. Attachments can damage your computer, or even enable outsiders to take control of it. Some hackers take control of others' email accounts and send out emails with dangerous links or attachments, so be careful even of emails from family and friends, especially if it doesn't really sound like them.

- For the same reason, never accept an offer sent to you by unsolicited email, even if it is something you really want. If you do want it, go on your own (but *not* by clicking an email link) to the website offering the product or service, and purchase it from there. If there isn't such a website, or a toll-free number, or some other legitimate way for you to find them, assume it is a scam – and look for someplace else to buy that product or service.

- *Never* click on a link unless you are sure it is valid. Some links don't go where they say they go, and clicking them can open up your computer to invasion.

- It generally *is safe* to give your credit card information over the internet to legitimate businesses, especially if it is a "secure" site. Up-to-date web browsers will warn you if you are dealing with a non-secure site. In general, web addresses that begin with "https:" are secure for financial transactions (that's what the "s" stands for). Furthermore, credit card companies *want* you to use their cards over the internet, so in the rare event that an on-line transaction leads to fraud, they will almost always cover you for it.

- But do not respond to emails, especially those purporting to be from banks, other financial institutions, or popular auction or retail sites, if they are asking you for personal or financial information. These are almost always illicit attempts to get you to reveal information that will be used to harm you. This practice is called "phishing," and legitimate companies rarely do business in this fashion. Assume that all such requests are scams. If you suspect that a particular case (for example, from an internet auction site) might be OK, make sure that the details correspond to a transaction that you have already voluntarily taken part in. If you have any doubts, call the company's toll-free number to see if there is a real problem or not (but *not* a number provided in the email itself – check your most recent statement, or find the number in a phone book or online).

- Don't fall for investment tips you find on the internet – especially on blogs, bulletin boards, online investment newsletters, or in your email. Con artists buy stock in small companies, then tout them to other people, like you, who also buy them

and drive up the price. Then the con artist sells, and you and everyone else who bought it loses out as the artificial price boom ends and the price drops.

In person:

- It may shock you to learn that in a 2012 survey of regulators and other professionals, the most commonly identified fraud problem was theft or diversion of funds or property *by family members*, with theft or diversion *by caregivers* coming in second, and financial scams *by strangers* third. What can you do? Consider having a financial professional (accountant, lawyer, financial advisor) be a co-trustee with any family member or caregiver who is given authority over your money. And remove or lock up valuables if you or an elderly relative will be home alone with a caregiver.

- The next most common in-person frauds are door-to-door sales, often for home improvements, but sometimes for random goods. Not all such offers are fraudulent of course, but many are, so you should always ask for a business card or phone number, and tell them you will call them back (after you check around to see if their terms are reasonable). If they refuse, and say ñthey just happened to be in the neighborhoodò or give some other reason why you canôt get the same deal tomorrow, assume itôs a scam and send them on their way.

- Some con artists will try to get to know you, or perhaps a group of people including you, looking for the right opportunity. This is called ñaffinity fraud.ò It is harder to be properly suspicious with someone you have known for a while, and who perhaps has shown a lot of interest in you and really seems to care. So what do you do? Always be business-like about business matters ï even (especially!) with a close friend or family member. *All financial transactions should be documented*. Agreements should be expressed in writing, and signed by both parties, with copies provided to both parties. Cash transactions should be accompanied by signed receipts. Such procedures protect all parties ï as well as those left behind if one of the parties dies or becomes disabled.

- Even if your best friend made a killing ñinvestingò with someone, it doesnôt mean you will. So-called Ponzi Schemes are set up to work just that way: a few people are given extraordinary returns early on, which are paid for by getting more people to ñinvestò based on these early successes. In most cases, there isnôt even any investment being made. The con artist pays out some of the money to the early contributors, to generate excitement, but then keeps the rest. By the time you hear that someone else has made money on the scheme, itôs already too late for you ï youôre going to lose all of yours, if you contribute.

- Home care workers are generally honest, but then again, itôs a great opportunity for someone who is not honest. If you need to bring someone new into your home, pay to have a background check done. And it is best if they are bonded, or if they work for a company that will make good on any theft or other problems.

**If you suspect you are being scammed:**

- Check on the person or company involved, using independent means.
- Inquire with the Better Business Bureau, your state Attorney Generalôs Office, the local police, and/or your stateôs consumer protection agency.
- Newspapers and television stations often have consumer fraud reporters or investigative units ï they might already know about the scam, or might be interested in doing a story on it.
- See the notes at the end of this paper for further advice for certain kinds of fraud.

**If you have been scammed, or your identity has been stolen:**

- Admit to yourself that youôve been tricked. This can be hard, but chances are you were up against a professional, so you donôt need to be all that embarrassed. If you take action, you might be able to save the situation: perhaps get some or all of your money back, and just as important, help assure that the culprit will be less able to do the same thing to other people in the future.
- Immediately contact your credit card company, bank, and/or other financial providers that carry accounts of yours that might be affected. Credit card companies can immediately cancel an account (and usually replace it with a new one), and banks can stop payment on checks, or disable access to existing accounts.
- Contact the agencies mentioned in the previous section, and/or see the notes at the end of this paper for online reporting of some specific kinds of fraud.
- If you suspect (or know) that your credit rating has been affected, you are entitled to a free credit report, and can notify all credit bureaus of the fraud with a single phone call to any one of them.

**What if a legitimate business or insurance company is treating you badly?**

The Consumers Union suggests several steps you can take:

- Speak to the boss, and the bossôs boss, and the company CEO, if necessary.
- File multiple complaints at the same time, to consumer, business, and state government watchdogs.
- Go to federal agencies, such as the Federal Trade Commission.
- Complain to the Better Business Bureau, and to organizations that represent the industry the offending company belongs to.
- Get a lawyer, who may send a more threatening ñletter of demand,ò or even, perhaps, file a lawsuit. An experienced attorney can advise you on the best course.

## For More Information

- ***General information:***
  - Check out: http://www.fraud.org/ for a wealth of good information, especially about telemarketing and internet fraud.

- The National Council on Aging, working with Bank of America and the Womenôs Institute for a Secure Retirement, offers a booklet available in PDF form titled Savvy Saving Seniors: Steps to Avoiding Scams, for free, at: http://www.ncoa.org/assets/files/pdf/savvy-saving-seniors/Savvy-Saving-Seniors-Participant-Handbook-FINAL.pdf
- The North American Securities Administration Association (NASAA) has detailed information about investment fraud ï how to spot it, prevent it, and deal with it after it happens. Go to: http://www.nasaa.org/1723/senior-investor-resource-center/.
- The U.S. Securities and Exchange Commission offers tips on questions to ask about investments, and about identifying fraudulent investment offers over the internet. They also have a page on Affinity Fraud, and a list of recent/current scams in this category. Go to: http://www.sec.gov/investor/seniors.shtml.

- ***Helping your elderly parents or others deal with fraud issues:***
  - Visit the AgingCare.com website on ñFrauds and Scamsò: http://www.agingcare.com/Frauds-Scams.
  - Kimberly Lankford, ñHow to Protect Parents from Elder Investment Fraud,ò at the Kiplinger website (http://www.kiplinger.com/columns/ask/archive/how-to-protect-parents-from-elder-investment-fraud.html)
- ***If you suspect identity theft, or want to prevent it:***
  - Visit the Federal Trade Commissionôs identity theft website: http://www.ftc.gov/bcp/edu/microsites/idtheft/.
  - Visit the Justice Department site on ñIdentity Theft and Identity Fraudò: http://www.justice.gov/criminal/fraud/websites/idtheft.html
  - Read the Federal Reserve Bank of Bostonôs pamphlet on *Identity Theft*, available online at: http://www.bos.frb.org/consumer/identity/idtheft.pdf.
- ***Checking out a financial advisor's credentials:***
  - Registered investment advisors are listed with the Financial Industry Regulatory Authority (FINRA). For more information and assistance, visit their ñProtect Yourselfò page at http://www.finra.org/Investors/ProtectYourself/. The Securities and Exchange Commission also offers help about investment firms, at: http://www.adviserinfo.sec.gov.
  - The NASAA site helps you find your state regulator, who may have additional information: http://www.nasaa.org/about-us/contact-us/contact-your-regulator/.