

Avoiding Fraud: Tips for Individuals*

Jeffrey D. Oldham

2009-10-23

Abstract

Fraud is an intentional deception made for personal gain or to damage another individual. Deceptions or scams abound, trying to deceive ordinary people. The types of fraud are too numerous and change too quickly to list, but we describe present categories of fraud and the common underlying elements. From the point of view of an ordinary American resident, we describe how to minimize the chance of deception and how to decide if an opportunity is a deception. We do not present proper legal actions after being defrauded.

1 Fraud

Fraud is an intentional deception made for personal gain or to damage another individual. The list of all types of fraud is too long to list, but some include

- false billing where a fraudster sends a bill for some product or service that has not been provided hoping the recipient will pay the bill,
- tax fraud such as not paying one's taxes by hiding it abroad or using illegal tax shelters, and
- Ponzi schemes.

The extent of fraud is large but not currently measured, and there is not even a standard definition [Gen06, Ch 2]. One estimate is that fraud costs £20 billion annual loss in the United Kingdom, i.e., about £330 per year per man, woman and child [LBF⁺07, Foreword].

Since it is not currently measured, its growth rate is difficult to measure. The growth of the internet, facilitating anonymous contacts among geographically remote people, may be increasing the number of frauds.

During every day, most American residents receive information from hundreds or thousands of sources. We receive emails, watch television shows and commercials, talk to neighbors, listen to the radio, read newspapers and magazines, receive

*©2009 Jeffrey D. Oldham (oldham@cs.stanford.edu). All rights reserved. This document may not be redistributed in any form without the express permission of the author.

letters delivered by the postal carrier, see billboards, and interact with classmates, officemates, and strangers. A scammer can use all these ways of communication. Eliminating all communication would eliminate the chance of being defrauded, but, as social creatures, humans need communication to enjoy life. Instead, we reduce the communications a scammer is most like to use, minimizing the probability of receiving deceptive information. For example, one can ask the Direct Marketing Association to have its members not send junk mail.

When presented with information, we can use common characteristics of fraud to decide whether the information is likely to be deceptive or not. For example, many frauds involve a person with whom you have not previously communicated, secret or proprietary information, or the ability to make money fast. If there is still some doubt, further investigation might be warranted. For example, one can check a person really is calling from the San Francisco Police Department by finding its main number, perhaps using a search engine, and then asking to be transferred to the original caller.

No matter how careful, everyone is defrauded occasionally so victims should not feel guilty or stupid because of fraud. Report the fraud to the appropriate authorities as quickly and as completely as possible. This document does not address how to do this.

1.1 Caveats

Fraud is not the author's area of expertise, and the area of fraud is too large but too fragmented to perform an adequate survey with reasonable effort. Comments and suggested improvements are solicited.

2 Definitions of Fraud

There are no universally accepted definitions of fraud. In preparation for the creation of the United Kingdom's Fraud Act of 2006, some reports defined *fraud* as

causing loss or making a gain at the expense of someone by deception and dishonest means [Gen06, 2.4]

and

the obtaining of financial advantage or causing of loss by implicit or explicit deception; it is the mechanism through which the fraudster gains an unlawful advantage or causes unlawful loss. [LBF⁺07, ch2], [LB08, p. 299].

The U.K.'s Fraud Act of 2006 [Eli06, §§2–4] defined three categories of fraud paraphrased here:

- A person commits *fraud by false representation* if he dishonestly makes a false representation.

- A person commits *fraud by failing to disclose information* if he dishonestly fails to disclose to another person information which he is under a legal duty to disclose.
- A person commits *fraud by abuse of position* if he occupies a position in which he is expected to safeguard, or not to act against, the financial interests of another person and dishonestly abuses that position either through acting or not acting.

For all three cases, the person must also intend to make a gain for himself or another or to cause loss to another or expose another to a risk of loss.

All three types require dishonesty, and acting or failing to act is also required. Seeking advantage over another is also required. The fraudster can seek gain in property, whether physical or not, permanent or temporary, or the fraudster might just seek to cause loss to others. The definition applies to both individuals and to companies and company officers.

In the United States, each jurisdiction, e.g., federal, state, county, or city, defines its own set of frauds. There is no generally accepted legal definition. A South Carolina Court of Appeals decision listed nine required elements for fraud to occur although the opinion was clearly marked as not providing precedent [Mor09]:

- a representation,
- its falsity,
- its materiality,
- knowledge of its falsity or a reckless disregard for its truth or falsity,
- intent that the representation be acted upon,
- the hearer's ignorance of its falsity,
- the hearer's reliance on its truth,
- the hearer's right to rely thereon, and
- the hearer's consequent and proximate injury.

Although including dishonesty and a motive, the requirements omit the fraudster's seeking gain or avoiding loss.

2.1 Categories of Fraud

Fraudulent activity manifests itself in many different ways (and therefore lends itself to different sub-categorisation in the way other crimes do not). [Gen06, 2.5]

The different kinds of fraud are numerous and change through time. Instead of including an incomplete list, we present categorizations of fraud [Hay02].

- simple misrepresentation. For example, claiming that the U.S. income tax is illegal and presenting a scheme to not pay taxes is simply incorrect since the U.S. Constitution's Sixteenth Amendment permits income taxes.
- the Spanish Prisoner. The fraudster confidentially contacts his victim, indicating a wealthy person has been imprisoned in Spain under false identity. If the victim supplies some money to release the prisoner, he will be handsomely rewarded. Of course, the money is accepted, but the prisoner is never released [Wik09d]. Nigerian spam emails asking for money to cover expenses to release the bank account of a deceased relative are a modern variant [Wik09a]. Key features of this fraud include secrecy, confidence in not revealing the Spanish Prisoner's condition, soliciting money, and the promise of future great wealth.

The fraud was named from a short story by Arthur Train [Tra10].

- Ponzi schemes. The fraudster offers an investment opportunity paying high returns. Initial investors are paid using money received from subsequent investors. The scheme collapses when investors stop supplying additional money or the fraudster disappears.

Key features include the opportunity to make higher than normal returns without an underlying economic model to do so. The scheme may be publicly known.

The fraud was named for Charles Ponzi who conducted a large Ponzi scheme in 1920 [Wik09b].

- pyramid schemes. A scheme consists of recruiting people who pay money to those already in the scheme. Recruits are typically promised large amounts of money from the people they recruit. Each person receiving money pays money to his recruiter. The scheme collapses when new people cannot be recruited.

Key features include continually recruiting new members and having no true underlying economic value.

In 1997, the entire Albanian economy collapsed from banking pyramid schemes where businesses even promised to double an investment in three months [Jar00] and sparked political unrest called the Lottery Uprising.

Multi-level networking businesses such as Amway *may* be distinguished from a pyramid scheme because real products are delivered. Ponzi schemes may also have a pyramid structure.

- shell games. A canonical shell game involves three shells and a small ball. After shuffling, if the victim chooses the shell having the ball under it, the victim wins. Through slight of hand, the fraudster can ensure the victim never wins. Sometimes collaborators egg on the victim or give some inside information how to win. The term can be generalized to an apparent game of chance which a fraudster instead controls.

Key features include the appearance of a game of chance when the outcome is actually determined.

Called the thimberig game, the fraud was mentioned in the 1670 book *Hull Elections — Richard Perry and His Fiddler Wife* [Wik09c].

- uncommon opportunities. The fraudster presents a way to make more money than is usual given the required effort. For example, one can earn CEO-level money while working at home, get rich trading stocks from home, or conduct insider stock trading.

Key features may include joining the secret group or the “inside group” and some secret knowledge. Payment of money or information, e.g., address or bank account numbers, can be required before obtaining the secret. A scheme’s existence be publicly advertised but usually its secret knowledge is not.

2.2 Examples of Fraud

The list of all possible frauds is too long and changes too rapidly to include a complete list. We illustrate a few from [LB08, Table 1] plus a few more.

- benefit fraud
- billing fraud
- charity fraud
- check fraud
- consumer frauds, e.g., lottery scams, misleading products, gaming frauds
- counterfeit products
- counterfeit money
- data-compromise fraud, e.g., phishing and pharming
- embezzlement
- gaming frauds
- insider dealing
- insurance fraud
- investment fraud
- lending fraud including fraudulent bankruptcy and mortgage fraud
- mail fraud
- payment card fraud

- pension-type fraud
- procurement fraud
- tax fraud
- wire fraud

2.3 Frequent Characteristics

Despite the numerous types of fraud, many frauds have similar characteristics, which can be used to identify them as frauds. They include:

avoiding checks and balances: A fraudster may avoid inclusion of any third party or any tracking. For example, a fraudster may require cash, not a check, or may refuse to give verifiable contact information.

avoiding details or fine print: A fraudster may brush off detailed questions or defer them for later discussion. In fact, there may be no details because nothing is truly being offered.

better than average: A fraud may involve an opportunity to do better than average, e.g., a higher rate of return without additional risk; to get ahead faster, e.g., earn CEO-level money while working at home; or be too good to be true, e.g., obtaining a lottery payment if only you pay a processing fee.

involving an unknown person or company: Since most schemes are revealed to be frauds when they are completed, a fraudster must be able to end all interaction when the fraud ends. Thus, a career fraudster is likely to be previously unknown to the victim.

involving money: The goal of most frauds is to obtain property, and money is an easy way to exchange property.

lacking economic value: Some schemes have no underlying economic value to anyone involved except for the fraudster. If everyone in the world participated, would anyone's needs be fulfilled?

limited duration: An opportunity may be available for a limited time only, reducing the time to think about and question the opportunity. This can appeal to most humans' more regretting a loss (of opportunity) than a gain.

secrecy: Frauds use secrecy both to entice people and to prevent detection. A fraudster may claim to know a secret that will be revealed to a select group of people, appealing to the human desire to be wanted to and to be exceptional.

A fraudster may use secrecy to avoid detection. For example, someone's life or property will be in danger if the transaction is revealed too early. Or the scheme should not be discussed with one's spouse. An isolated person is more easily victimized.

uninitiated contact: People seldom seek out frauds. Instead fraudsters usually initiate contact.

Although fraud is illegal, illegality may not be usually initially discernible.

3 Minimizing the Chance of Possibly Fraudulent Schemes

Much fraud can be avoided if consumers, businesses, and public sector bodies took elementary precautions and, in appropriate circumstances, exercised sensible scepticism about offers that were obviously too good to be true. Prevention must be the first step we take. [Gen06, Foreword]

Unless one stops all physical contact, it is impossible to avoid contact with fraudsters. However, one can reduce the number of possibly fraudulent schemes for which one has to determine if it is fraudulent or not.

3.1 Reduce Unsolicited Communication

Because many frauds are not initially solicited, reducing the ways untrustworthy people can contact you.

reduce unwanted physical mail: Opt out of most junk mail by registering your address with the Direct Marketing Association Mail Preference Service at <https://www.dmachoice.org/dma/member/regist.action>. Reputable mail-order companies are members of this organization. Non-reputable ones are not. Separate junk mail cessation lists for deceased individuals and dependent individuals are available.

Avoid giving out your contact information except where necessary. For example, entering a lottery is a poor way to win money but a great way to get more junk mail.

Notify mailers you wish to be removed from their mailing lists. When receiving junk mail, mail the enclosed prepaid envelope or a postcard stating “Per federal law, remove my address from all your mailing lists.”

Mail a letter to each of the three major credit bureaus stating you do not want your personal information shared for promotional purposes. See the FTC site listed below.

Also, you can opt-out of unsolicited credit and insurance offers by calling 888-5-OPT-OUT or visiting www.optoutprescreen.com.

reduce unwanted phone calls: Register with the National Do Not Call Registry by visiting www.donotcall.gov or phoning 888-382-1222. Political organizations, charities, and “surveyors” may still legally call, but you can tell them,

“Per federal law, do not contact me again.” Unreputable or uninformed solicitors will state that they are not covered by the Do-Not Call List; just restate your request and hang up.

reduce unwanted email: Only distribute your email address to people from whom you want email. For example, do not enter your email address into random web forms.

Register your email address with the Direct Marketing Association’s email Preference Service (eMPS) available off <http://www.dmachoice.org>.

When registering at website, be sure to opt-out of receiving emails.

Reputable companies will remove your email address from their lists upon request, but unreputable ones will use this information to sell your email address since it has proven to be active.

Use a good spam email filter. If you receive more than one spam email per day, choose a better spam filter.

reduce unwanted solicitations: Place a “no solicitors” sign outside your door, and do not open your door to solicitors.

The Federal Trade Commission also provides some tips at <http://www.ftc.gov/privacy/protect.shtm>.

3.2 Authenticate

Since much fraud involves contact by an unknown person or company, authenticate any communication, whether in person or not.

Reputable physical mail typically uses first-class postage, has a return address, and lists multiple ways to contact the organization. Use web search to confirm the organization’s address matches that listed on its website.

Reputable companies will not request private information via unsolicited phone calls. Instead, take the person’s name and company, use web search to find and dial the main phone number, and ask for the person. For example, if a person who claims to be from the San Francisco Police Department calls, take the person’s name and call back using the main San Francisco Police Department phone number, which can be found using a simple web search.

Do not click on links inside emails. Instead go to the organization’s main website and navigate to a particular page. Some emails may direct to misleading sites.

If a person claims to represent a particular company, take the person’s name and contact the company directly using a means not given by the person. For example, if an unsolicited Comcast serviceperson arrives at your door and wants entry, ask for the person’s name and call the toll-free number on your most recent Comcast bill. If you are not a Comcast subscriber, assume the person is a scammer.

4 Is the Scheme Fraudulent?

Even after minimizing the chance of being presented with a possibly fraudulent scheme, almost everyone will occasionally still have to decide whether a particular scheme is fraudulent. The frequent characteristics of frauds and the types of fraud in Sections 2.3 and 2.1 may help make a definitive decision. If you have doubt, assume it is a fraud.

Because most fraud are illegal and many involve secrecy, involving other people can be helpful. If the schemer discourages having someone else help you with participation, e.g., because it is an exclusive scheme or there is no time, it is probably a fraud. Involving other people helps ask questions like whether the proposal has any true economic value. Just asking questions may be enough to discourage a fraudster; however, some fraudsters may try to get a victim to talk to form a relationship so be wary.

Performing web searches can reveal more information about the proposed scheme. For example, the author regularly performs web searches to determine that mass-mailing emails are actually frauds. For example, the author received an email stating there was a bill to give illegal aliens Social Security privileges. Using a web search engine to search for “illegal aliens Social Security” yielded suggested searches of “illegal aliens Social Security hoax” and “illegal aliens Social Security site snopes.com” indicating the email was fraudulent. Web search engines try to provide the most relevant results so, if a scheme is a hoax, the hoax result is likely to be ranked highly.

A legitimate company will permit a potential customer to spend enough time collecting information and also wait to purchase. If you are pressured to purchase, it is probably a fraud.

If you have not previously heard of the person or company offering the scheme, think whether you would know how to find the person or company if you do not use the provided contact. For example, if a person gives only a post office box and no phone number or website, the person can disappear by just closing the postal box. It’s probably a fraud.

Determine if there are any outstanding or previous complaints against the individual. Brokers, contractors, mechanics, and many other people and also companies are regulated by state government. Ask for a license number and use web search to find the person’s history.

Avoid giving out your private information unless you initiate a transaction. For example, no one should ask for your Social Security number except for income-tax related reasons. Unfortunately, the medical industry also uses Social Security numbers despite its being against federal law.

5 Recovering from a Fraud

These precautions are not going to stop all fraud; fraudsters will always manage to deceive some people and businesses. [Gen06, Executive Summary 2]

Even the most vigilant person will fall victim to fraud occasionally. There is no shame in being a victim. Do report the fraud to the appropriate authorities as soon as possible. Unfortunately, recovering from fraud is beyond the scope of this document.

References

- [Eli06] Elizabeth II. Fraud Act 2006. http://www.opsi.gov.uk/acts/acts2006/pdf/ukpga_20060035_en.pdf, November 2006.
- [Gen06] United Kingdom Attorney General. Fraud review. <http://www.attorneygeneral.gov.uk/Fraud%20Review/Fraud%20Review%20Final%20Report%20July%202006.pdf>, London, July 2006.
- [Hay02] Teresa Nielsen Hayden. The underlying forms of fraud. <http://nielsenhayden.com/makinglight/archives/001509.html>, October 2002.
- [Jar00] Christopher Jarvis. The rise and fall of albania's pyramid schemes. *Finance & Development*, pages 46–49, March 2000. <http://www.imf.org/external/pubs/ft/fandd/2000/03/pdf/jarvis.pdf>.
- [LB08] Michael Levi and John Burrows. Measuring the impact of fraud in the UK. *British Journal of Criminology*, 48(3):293–318, February 2008.
- [LBF⁺07] Michael Levi, John Burrows, Matthew H. Fleming, Matthew Hopkins, and Kent Matthews. The nature, extent and economic impact of fraud in the UK. <http://www.attorneygeneral.gov.uk/attachments/ACP0%20report%20-%20The%20Nature%20Extent%20and%20Economic%20Impact%20of%20Fraud%20in%20the%20UK.pdf>, February 2007. Association of Chief Police Officers' Economic Crime Portfolio.
- [Mor09] 2009-up-002: Morlan v. Kelly. <http://www.sccourts.org/opinions/displayUnPubOpinion.cfm?caseNo=2009-UP-002>, January 2009.
- [Tra10] Arthur Train. The Spanish prisoner. *The Cosmopolitan*, 48:465–474, 1910.
- [Wik09a] Wikipedia. Advance-fee fraud — wikipedia, the free encyclopedia, 2009. [Online; accessed 20-October-2009].
- [Wik09b] Wikipedia. Charles ponzi — wikipedia, the free encyclopedia, 2009. [Online; accessed 22-October-2009].
- [Wik09c] Wikipedia. Shell game — wikipedia, the free encyclopedia, 2009. [Online; accessed 22-October-2009].
- [Wik09d] Wikipedia. Spanish prisoner — wikipedia, the free encyclopedia, 2009. [Online; accessed 20-October-2009].