Uncovering Fraud, Before It Buries You.

By Barry Minkow

INSIDE THIS ISSUE

1 Recognizing Fraud
2 Avoid Investment Fraud
3 Hang Up On Telemarketing Fraud
5 Boom Gone Bust: Elder Fraud
7 Safety In Numbers: Affinity Fraud
12 I Think I've Been Scammed. Now What?
17 Be Your Own Investigator

BARRY MINKOW PRESENTS THE INVESTOR PROTECTOR SERIES BARRY MINKOW PRESENTS THE INVESTOR PROTECTOR SERIES BARRY MINKOW PRESENTS THE INVESTOR PROTECTOR SERIES BARRY MINKOW PRESENTS THE INVESTOR PROTECTOR SERIES BARRY MINKOW PRESENTS THE INVESTOR

The INVESTOR PROTECTOR

Recognizing Fraud

Before you invest, investigate

Articles on fraud prevention usually begin with some sage advice about, "If it sounds too good to be true, it probably is." Unfortunately, many of us are inexperienced at investing, or we started to pay attention to our savings only as we neared retirement age. It can be difficult to know what "too good to be true" means.

A concrete example might help. Warren Buffett is regarded as being one of the most brilliant investors alive, and he is currently the second richest man in the country. Over several years, his average return on investment was 24% annually. So if you're considering an offer that promises more than 24% annually, it should raise some red flags for you.

Investments that promise high returns will also carry more risk.

Of course, sometimes an offer may contain more conservative promises and still be fraudulent. The best way to be sure is to look into the industry itself... see what kinds of returns are typical in that sector. For instance, technology investments can provide very high returns, but usually they also involve a lot of risk. That's another good rule of thumb: investments that promise high returns will also carry more risk than, say, a savings account, IRA, or bond.

Before investing in an opportunity, playing a lottery, or accepting an offer made by mail, e-mail, or telephone, do your homework. Use an Internet search engine like *www.yahoo.com*, *www.google.com*, or *www.ask.com* to gain information on the company, person making the offer, etc. You can look up things like addresses and telephone numbers, names of officers in the company, etc. Reputable businesses will usually leave an extensive "trail" online that lead you not just to their own Web site but also to press releases, newspaper articles, photos of corporate events, etc.

Check with your local Better Business Bureau, your State Attorney General's office, and local consumer groups to see if there have been any complaints against the company. Have a trusted family member, financial advisor, or friend look over the information and help you to evaluate it. It's important that anyone you ask for advice should not stand to benefit from your investment or acceptance of the offer... they could be an unwitting accessory to the fraud, without even knowing it.

Avoid Investment Fraud

Verify claims

Before investing any monies, ask the person or company offering the financial product the following simple questions:

What products or services are you offering? These could be insurance, estate planning, investments, annuities, securities, living trusts, or legal services. Be sure that you know what specific product or service is being offered, so that you can investigate this type of offer.

Who regulates or licenses this type of product/service? Any type of offer that takes your money and promises a return on that money will be regulated and/or licensed by state organizations like the State Bar, Department of Insurance, Department of Corporations, Department of Real Estate, Board of Accountancy, etc. If someone tells you that "this type of investment is licensed or regulated," that should be another warning flag for you.

If they claim to have a securities license, real estate license, CPA certification, etc. then ask them to provide a copy of that license for your records. Legitimate brokers will not be put off by this request and will be happy to provide their credentials.

What is the address, telephone number, fax number, Web site, etc., for the company making the offer? Be sure to obtain a complete postal mailing address, not just a Post Office Box. Legitimate businesses will have telephone numbers, fax numbers, Web sites, and e-mail contacts. Obtain all of these, and be wary of anyone who attempts to conceal any part of this information.

Now that you've obtained this information, inform the person making the offer that you will need time to verify the offer. If they pressure you to invest immediately, or make claims that the offer is for a limited time only, again this should cause concern.

Call the state licensing board or department to verify the company or individual. Perform the Internet searches recommended earlier. Remember: legitimate businesses will leave an extensive "trail" on the Internet, not just one slick-looking Web site. Beware of Web sites that look nice, but have little real "meat" or content. These are often the mark of hastily constructed scam sites or false fronts used by con men.

You worked hard to make your money, so take the time to do a little homework to protect it. In the end, it will pay off in your own peace of mind. There is always an element of risk in any investment, but by being certain that both the offer and the broker are legitimate, you can avoid the risk of fraud.

Peace of mind is the best return on investment of all.

Hang Up On Telemarketing Fraud

Giving con men the busy signal

We've all had these annoying calls, interrupting the dinner hour or a favorite television show. The reason why there are so many of them is simple: they work. Unfortunately, this fact was quickly grasped not only by legitimate companies, but by con men as well.

The telephone provides one thing that is usually critical to make any scam a success: a degree of anonymity. One guy operating out of his spare bedroom can sound just as large as any Fortune 500 company. These con men have even figured out how to change their "Caller ID" listing to make themselves look more legitimate. Add a wife or girlfriend willing to play the part of "secretary" and these back-room operations can sound pretty impressive.

Another wrinkle that con men have stolen from their legitimate telemarketing counterparts is the use of so-called "boiler rooms." Hundreds of operators may man these phone banks, allowing them to target thousands of potential victims per hour. For every hundred people who hang up, they may only get one "fish" who takes the bait, but that is more than enough to make the con men rich.

Sometimes the operators who man these banks are fully aware of the scam; other times, they are innocently helping to bilk people of their savings without even being aware that a crime is being committed.

What can I do to avoid this type of fraud?

FTC Do Not Call Registry
1-888-382-1222
www.donotcall.com

The Federal Trade Commission found that unsolicited calls and fraud were such a huge problem for consumers that they took extraordinary steps to help protect them. Using the "Do Not Call Registry," it is possible to block most forms of telemarketing calls.

The first step in preventing these types of fraud is to have your own telephone number and that of your loved ones "blocked." You can do this in two ways:

By Telephone: Call 1-888-382-1222 and follow the simple prompts to sign up.

By Internet: Visit *www.donotcall.gov.*

Registration for this service is free. The block can take three months to go into effect, but after that time you should only receive calls from a few types of groups that were exempt from the federal regulation.

If after subscribing to the Do Not Call Registry you receive telemarketing calls, simply tell the caller, "This number is on the Federal Trade Commission's Do Not Call

Registry. Please remove this number from your list. If you call again, you will be reported to the FTC." And then hang up! It's that simple.

I signed up for the Do Not Call Registry months ago, but I continue to receive calls from companies that say they are exempt. What should I do?

Placing your number on the National Do Not Call Registry will stop most, but not all, calls. Political organizations, charities, and telephone surveyors are still allowed to call your number.

Companies with which you have an established business relationship can call you for up to 18 months after your last purchase, payment, or delivery even if your number is on the Do Not Call Registry. And companies to which you've made an inquiry or submitted an application are allowed to call you for three months. You should carefully read any questionnaires or surveys you submit; these may be an attempt to establish a business relationship. Be careful to read anything you sign, such as offers for "free" products... sometimes the price of this product is establishing a business relationship with that company, so that they are free to call you again.

As always, the best advice for avoiding any calls you don't want is to tell the caller firmly, "I don't wish to talk to you. Please do not call again." And then hang up.

I'm worried about my parents. They are easily confused by calls like these – what can I do to protect them?

First of all, you're to be congratulated for being concerned about your parents and their financial security. Too often adult children don't pay attention to things like this, until it's too late.

The first step is to tell your folks about the FTC Do Not Call Registry. Get their permission to add their telephone number to the list. Also, talk to them about the dangers of accepting offers over the phone, and encourage them to discuss any calls that they don't understand with you, before they take any other action.

But if these guys are crooks, what guarantee do I have that they will respect the Do Not Call Registry?

Great point! The answer is that you have no reason to expect that they will even bother to obtain the registry, much less avoid calling people who want their number blocked.

But having your number on the list can act a warning signal to you. If you receive a call from a company that is not a charitable organization or political organization, then you should suspect fraud.

If you've told this caller that your number is on the registry, and they continue to call, then you should not only be wary, but also report them immediately to the FTC using the toll-free number or Web site listed earlier.

OK, I've taken your advice. Is there anything else that I should look out for?

Yes. As a consumer you should realize that telemarketing is now an established form of sales, with almost two decades' worth of research to refine its pitches.

Many forms of sales pitches are legitimate, but still deceptive. For example, say that you decide to order a product from an advertisement on television. We'll use a collection of "oldies" music for our example. You call and order the recordings and pay with your credit card. Sounds simple, right?

At this point, the operator will likely begin a series of "up sell" attempts. Reading from a number of pre-formatted scripts, they may offer you similar items at a reduced price, or other products that their research has told them you're likely to want.

This type of selling is not illegal, but often there are hidden catches. For example, an additional CD may be priced at only $4.99 plus the additional shipping and handling charge. Sounds good, right? But what if the shipping and handling charge is $7.99?

As a consumer, you have to be informed of these types of sales techniques and not agree to any offer without knowing the full details. If you reject the first "up sell" offer, the operator will likely continue to ask you about other products or services. These are high pressure tactics, designed to maximize the company's profits on your phone call. They know that this may be their only opportunity to reach you, and after spending a lot of money on that television ad, they want to be sure that they take maximum advantage of the call.

Another technique is the "work around," in which the operator may ask you if it's OK for them to contact you about similar products or "special offers" in the future. If you say yes to this one, you'll be in line to receive a lot more calls from this company for the next three months. Also, be careful about giving out your e-mail address for the same reason.

The next time that "opportunity" calls, rather than knocks, be prepared to hang up. You may miss the chance of a lifetime, but more than likely you'll just hold on to more of your money.

Boom Gone Bust: Elder Fraud

Scam artists target those above 50 years old

It is a cliché that senior citizens are easy marks for con men – so much so that many victims do end up falling prey to fraud, simply because they don't see themselves as the typical "victim" portrayed in crime prevention messages.

In truth, the fastest growing segment of our population is the "baby boomers" generation, but instead of finding these boomers to be easy pickings, many con men are discovering that this generation is worldly, educated, and computer savvy.

But the boomers are also the most affluent generation in American history. Many are entering their retirement years with more total savings than their parents or grandparents could ever have dreamed of. This makes them an attractive target for fraudsters.

Adults who are nearing retirement age are also often looking for "golden opportunities" to pad their nest eggs before leaving work. While they're too wise to fall for the usual get-rich-quick schemes, many can be lured into investment offers if they are couched in the right way. Often these scams involve luring one or two members of a group into the investment, and rewarding them with unbelievable profits quickly. These members can then influence their friends or family to get involved... and these people are conned out of considerable sums.

With advancing age, health problems can also make seniors more vulnerable to fraud. For instance, high pressure techniques are sometimes effective, because the con man is able to simply wear down the victim with repeated phone calls or visits. It can be more difficult to read the fine print on contracts or written forms, and many seniors will simply sign the form if nothing seems amiss.

Cultural or generational differences can also be exploited. For many seniors, they remember with fondness a simpler time when business was conducted on a handshake and a promise. Con men who appeal to these types of values may be successful at getting a victim to ignore contractual details.

Some seniors lead solitary lives with limited social contacts. Children and grandchildren may live far away in other states, and downsizing to a smaller home often means that relationships with neighbors may be limited as well. Fraudsters can take advantage of this by spending hours just "getting to know" their victims. They engage them in friendly conversations, often with no pressure to buy or invest initially.

After the victim has established a relationship with a fraudster, they may be reluctant to upset their new "friend" and will invest a small amount of money, or make small purchases, to keep the con man happy. These usually escalate into larger and larger sums over time.

But the boom doesn't have to go bust, if seniors will recognize their special risk factors and take steps to avoid becoming a victim. Information is the best resource, and this DVD series is a great first step.

It's also important to involve your adult children, trusted advisors, or friends in important financial decisions. Never be embarrassed to seek assistance if you don't understand a complicated offer. If you're not a banker or investment broker yourself, then no one will expect you to understand it all, any more than they expect you to be able to fly a plane simply by reading about it.

And remember to use your best weapon: some old-fashioned common sense. That way, the Golden Years can truly be golden.

Safety In Numbers

Affinity fraud is the newest wrinkle on old scams

Law enforcement officials who protect consumers from fraud witness a never-ending series of new faces on some very old scams. They can see the underpinnings of a very old con, like a "Ponzi" scheme in the latest Internet stock scam.

Con men don't really dream up new scams, as much as they look for ways to re-engineer them for a new generation of victims. One of the fastest growing types of fraud is called "Affinity" fraud. According to the dictionary, affinity is a "relationship or kinship."

Churches, civic clubs, high school band boosters, and little league teams can all be targets for this type of fraud. So, too, can those groups which only exist in the "virtual world," like fantasy football leagues, or (online) clubs and communities.

The concept is simple. If offered an investment opportunity or product directly, you might dismiss it without really considering it at all. But if the same product or investment was offered by a trusted member of your group, you might be more likely to accept it, right?

Now imagine that a con man can manipulate the leader of your group or a very popular member into the investment. Perhaps they even trick this person into thinking that they're making a good return on that investment by sending them large checks of "dividends." The con man can then trade on that person's influence within the group to lure lots of new victims, often without their knowledge.

Affinity *n., pl. 1. A natural attraction: liking. 2. Relationship: kinship.*

In a nutshell, that's how affinity fraud works. It isn't a type of fraud, as much as it is a method of luring people into the scam. And because it is so successful, it's become one of the biggest threats out there.

So what can your group do to prevent becoming a victim of this type of scam? Below are some simple steps that you can take:

1. **Consider modifying your group's charter, rules, or policies to prohibit financial relationships between elected officers and members.** In legal terms, this is called a "conflict of interest," and it simply means that leaders of a group are obviously interested in the welfare of the group, and they're also human and like to make money. If you avoid situations in which the officers have to choose between these two desires, there will be fewer problems.
2. **Evaluate a product or investment based on its own merits, not on what anyone else might think of it.** This one sounds easy. But the truth is, we're all

still in jr. high in many ways. We want to be liked and accepted by the people we associate with, especially those that are leaders or are popular within the group. We have to recognize that fact and not allow it to cloud our financial decisions. Chances are that people within your group will continue to like and respect you regardless of your decision on any product or investment opportunity.

3. **Seek advice from someone outside the group before making a large purchase or investment**. Again, it comes down to recognizing that we're all human. Ask a family member, financial advisor, or friend who isn't part of the same group to look things over. Don't tell them any of the details of the group, just the facts about the offer. See what they think. Since they are outside the group, they'll be more objective.
4. **Don't mix business and anything else.** Many companies have policies against hiring family members (nepotism), or entering in financial deals of any type with family members and friends. It may be good advice. Just establish a strong personal policy that you don't like to mix business with other relationships. This provides an "easy out" on such offers, and most people will respect your decision.
5. **Consider their qualifications.** Just because your brother-in-law is a great softball player, does that also make him a financial whiz? Success is one area of life that doesn't always translate into other areas – maybe he really has hit on the opportunity of a lifetime, but what are the odds? If any offer sounds too good to be true, it probably is – regardless of who thinks otherwise.
6. **Special rules should apply to churches and religious organizations.** Our spiritual relationships are among our most treasured. Unfortunately, all types of evil have been done in the name of religion and fraud is no exception. Church leaders have a special responsibility to their members to protect them, and some additional information on strong polices are included for these groups within this booklet.

Churches and other non-profit groups should seriously consider revising their policy statements to include language that addresses the possibility of affinity fraud. Here are some guidelines to writing clear, policy statements that work:

The Ten Things All Affinity Fraud Policy Statements Should Contain:

1. **The spirit of the policy** – Non-profit organizations share four common goals with their members and regular attenders: vision, values, mission and message. No church or, for that matter, non-profit organization is established to generate large financial returns for participants but rather to provide much-needed spiritual refuge and encouragement. An affinity fraud prevention policy is designed as nothing more than a vehicle to protect people within the organization from people who would seek to use their affiliation with the

organization as an opportunity to take advantage of the vulnerable – not those who are vulnerable because they are naïve, but rather because they are inclined to believe claims made by those of the same faith, religious affiliation, race or group.

2. **What the target of the policy statement should *not* be** – (1) Legitimate financial planning services from Certified Financial Planners and other recognized experts in pre-approved contexts; (2) Tax advice and retirement planning from Certified Public Accountants and other recognized experts in a pre-approved context; (3) Debt counseling from approved experts in money management and debt reduction for those within the organization in need of this kind of assistance; (4) Legitimate church-approved (fund-raising) endeavors for special projects like building campaigns that often involve pledges.
3. **What the target of the policy statement *should* be** – Investment opportunities promising untenable returns, often guaranteed from individuals who are using their like beliefs or 'kingdom enhancement' promises to encourage investment. Also, multi-level marketing business opportunities which, may not be technically illegal, but still clearly create a conflict of interest, especially if staff or board members in the church are used by promoters to recruit others into the "company."
4. **The "why" behind the policy** – The Securities and Exchange Commission lists several cases that establish the seriousness and scope of the potential devastation of affinity fraud. The following four cases should be cited in the policy to anchor why such a policy is needed and supported by senior management and the board: (1) 125 members of various Christian churches lost $7.4 million – The fraudsters allegedly sold members non-existent "prime bank" trading programs by using a sales pitch heavily laden with Biblical references and by enlisting members of the church communities to unwittingly spread the word about the bogus investment. (2) Ponzi scheme targeted African-Americans and Christians – Defendants perpetrated an affinity fraud, raising at least $16.5 million from mostly African-Americans and Christians by falsely representing that they would receive returns through investments in, among other things, real estate, small businesses, and "markets of the world." (3) Baptist investors lost over $3.5 million – The victims of this fraud were mainly African-American Baptists, many of whom were elderly and disabled, as well as a number of Baptist churches and religious organizations located in a number of states. The promoter (Randolph, who was a minister himself and who is currently in jail) promised returns ranging between 7 and 30%, but in reality was operating a Ponzi scheme. In addition to a jail sentence, Randolph was ordered to pay $1 million in the SEC's civil action. (4) Trial is scheduled to begin in Florida for seven officials of the Tampa-based Greater Ministries International Church. They are

charged in a 20-count federal indictment alleging conspiracy, money laundering and mail fraud. State securities regulators and prosecutors believe Greater Ministries operated a massive Ponzi scheme that may have defrauded more than 17,000 investors nationwide of as much as $200 million. Many of the investors were fundamentalist Christians, including Mennonites in rural Pennsylvania, Ohio and Virginia. They were told their money would double in installment payments made over 17 months or less.

5. **Define terms** – Investment or business opportunities are defined as any instrument or endeavor – even the promise of someone "trading in the Forex or commodities markets" – that promises participants returns on investments but that requires the investor (participant) to rely solely on the expertise of the promoter in order to be successful in that endeavor.

6. **Communication** – There must be clear and consistent communication between all staff members, volunteers, lay leaders and board members on the education and implementation of any affinity policy, as the success of any policy is predicated on the "trench work" information gained by those closest to the action—lay leaders, volunteers and even support staff. They need to report any red flags about the promotion of a business or investment to no less than two people to avoid critical information slipping through the cracks.

7. **Paid church staff and board members should not, at any level, be involved financially with members of the organization without first securing permission from both senior management and the board.** There are two reasons for this: first, even in cases of legitimate business activities, like a member who is a real estate broker offering services to a staff person at a discount – there is a potential for danger – not because of fraud but because other real estate brokers who did not get the staff member's business may be offended. Second, promoters of illegal deals impute credibility to their 'offerings' by conveying who in the organization is 'in the deal.'

8. **Anytime someone within the church demands "secrecy" from others about what business investment or business opportunity they are promoting should be immediately reported to at least one staff person and one board member as secrecy is always a red flag for fraud.** Be especially wary if this "secrecy" is accompanied by the promoters reluctance to put the details of the investment opportunity in writing. This is why the proper communication of this policy to those who are most likely to hear about the latest promotions is critical, because they now can inform management of the potential danger.

9. **Obvious limitations of the policy** – Members and attenders can do business with one another outside the context of the organization (as long as they are not paid staff or board members). The purpose of this policy is limited in scope

to venues of the organization including, but not limited to, the organization's meetings and gatherings on or off premises and the organization's facilities and approved events being used as vehicles for the promoter to recruit or solicit those in the organization. Again, refer back to the first item listed about the shared vision, values, message and mission of the organization. Simply stated, the organization should not be an investment club.

10. **The more people that know of the policy, the better. Inform new members about this policy and explain that it is the board's only proactive method to prevent what is, sadly a common occurrence – affinity fraud.** The greater the number of people that are aware of this potentially devastating problem to the organization, the better chance senior management and the board have of avoiding financial catastrophe.

Below is a sample policy that can be formatted to fit the needs of the majority of churches and religious organizations. This sample is also available in an Adobe Acrobat and Microsoft Word format on this DVD. It can be easily modified in most word processor software.

SAMPLE AFFINITY FRAUD POLICY

This policy is being established with the specific intent of protecting members and attenders from any outside person who attempts to infiltrate the organization through befriending like-believing people of faith with the intent of recruiting investors for a particular investment or business opportunity.

All trustees, officers, agents and employees of this organization shall disclose all real or apparent conflict or dualities of interest that they discover or that have been brought to their attention in connection with this organization's activities. "Disclosure" shall mean providing properly, to the appropriate person, a written description of the facts comprising the real or apparent conflict or duality of interest. An annual disclosure statement shall be circulated to trustees, officers and certain identified agents and employees to assist them in considering such disclosures, but disclosure is appropriate and required whenever conflicts or dualities of interest may occur. The written notices of disclosures shall be filed with the Chief Executive Officer or such other person designated by the Chief Executive Officer to receive such notifications. At the meeting of the top governing body, all disclosures of real or apparent conflict or duality of interest shall be noted for the record in the minutes.

An individual trustee, officer, agent or employee who believes that he or she or an immediate member of his or her immediate family might have a real or apparent conflict of interest, in addition to filing a notice of disclosure, must abstain from:

(1) participating in discussions or deliberations with respect to the subject of the conflict (other than to present factual information or to answer questions),

(2) using his or her personal influence to affect deliberations,

(3) making motions,

(4) voting,

(5) executing agreements, or

(6) taking similar actions on behalf of the organization where the conflict or duality of interest might pertain by law, agreement, or otherwise.

At the discretion of the top governing body or a committee thereof, a person with a real or apparent conflict or duality of interest may be excused from all or any portion of discussion or deliberations with respect to the subject of the conflict.

A member of the top governing body or a committee thereof, who, having disclosed a conflict or duality of interest, nevertheless shall be counted in determining the existence of a quorum at any meeting in which the subject of the conflict is discussed. The minutes of the meeting shall reflect the individual's disclosure, the vote thereon, and the individual's abstention from participation and voting.

The Chief Executive Officer shall ensure that all trustees, officers, agents, employees, and independent contractors of the organization are made aware of the organization's policy with respect to conflicts or duality of interest.

I Think I've Been Scammed. Now What?

It's never too late to take control

One common reason that people seek out information about fraud is that they're concerned that they may already be a victim. If this applies to you, then the first thing you need to know is that you're not powerless. In fact, you may be able to turn the tables on the con men.

What should you do first? Don't invest any more money or purchase additional products or services until you can verify that the offer is legitimate. This sounds like common sense, but all too often con men are successful at milking even more money out of their victims, even after the victims begin to suspect fraud.

But don't rush to accuse anyone of fraud either. It's possible that you're mistaken and more importantly, you don't want to alert the bad guys that you're on to their scam. Just make excuses to delay them until you can check things out.

Then, begin to try to verify the offer and the salesperson. Check with your local police, Better Business Bureau, and state regulatory agencies that regulate the type of

business involved. Consider discussing the situation with a fraud prevention expert, like the Fraud Discovery Institute. **We can be reached toll free at 1-888-300-8307.**

Once you've confirmed that fraud is involved, your next step should be damage control. Ideally, you'd like to get your money back, but you should be aware that this rarely happens. So shift your focus to limiting the losses and their impact on your financial future.

Fraud is a crime, and like any crime, you need to report it. Ideally, you should report it to many different agencies, including your local police department, State Attorney General's office, the Better Business Bureau, and possibly the Federal Trade Commission or FBI. If the US Postal Service was involved at any point in the scam to send payments, sales documents, etc., then you should report the crime to the US Postal Inspection Service, which have some of the best anti-fraud investigators in law enforcement. Web sites for all these agencies are provided later in this booklet.

You don't want to alert the bad guys that you're onto their scam.

Make sure to get written copies of all reports submitted. You will need these later to verify your losses for insurance, credit history restoration, etc. If you have a choice, avoid automated (or online) reports, unless they provide a written copy of the final report for your records.

Your credit rating is very likely to be affected, especially in cases that involve identity theft. It's important that you immediately take the following steps:

1. Contact credit reporting agencies and ask to activate a "Fraud Alert."

Fraud alerts can help prevent thieves from opening any more accounts in your name. Call the toll-free fraud number of any of the three consumer reporting companies below to place a fraud alert on your credit report. You need only to contact one of the companies to place an alert. The company you call is required to contact the other two, which will place an alert on their versions of your credit report.

Equifax:
P.O. Box 740241, Atlanta, GA 30374-0241
1-800-525-6285 • ***www.equifax.com***

Experian:
P.O. Box 9532, Allen, TX 75013
1-888-397-3742 • ***www.experian.com***

TransUnion:
P.O. Box 6790, Fullerton, CA 92834-6790
1-800-680-7289 • ***www.transunion.com***

Fraud Alerts in more detail: There are two types of fraud alerts that you can request. One is an initial fraud alert that should be placed on your account if you

suspect identity theft. If you've been involved in nearly any type of fraud, there is the possibility that you have provided the con man with enough personal information to steal your identity. It's common for these crooks to share "mooch lists" that provide these details about their victims with other crooks. If you've been involved in nearly any type of fraud, you should place an initial fraud alert on your accounts. You can also request an extended fraud alert. Here are some more details:

- **An initial alert remains in effect for 90 days.** Request that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. When you place an initial fraud alert on your credit report, you're entitled to one free credit report from each of the three nationwide consumer reporting companies. Request those credit reports when you make the initial request for the alert.
- **An extended fraud alert remains in effect for seven years.** You can have an extended alert placed on your credit report if you've been a victim of identity theft and you provide the consumer reporting company with an "Identity Theft Report" from a local police agency or the FTC. When you place an extended alert on your credit report, you're entitled to two free credit reports within twelve months from each of the three nationwide consumer reporting companies.

Once you've confirmed fraud, your next step should be damage control.

In addition, the consumer reporting companies will remove your name from marketing lists for pre-screened credit offers for five years. This limits the damage that the crooks can do to your credit history.

To place either of these alerts on your credit report, or to have them removed, you will be required to provide appropriate proof of your identity; this may include your Social Security number, name, address and other personal information requested by the consumer reporting company.

When a business sees the alert on your credit report, they must verify your identity before granting credit. As part of the verification process, the business will try to contact you directly. This adds an extra layer of protection against additional credit accounts being opened without your knowledge.

2. Close the accounts that have been tampered with or opened fraudulently.

Call and speak with someone in the security or fraud department of each company. Follow up in writing, and include copies of supporting documents, such as the police reports that you've filed. It's important to notify credit card companies and banks in writing. Send your letters by certified mail, with return receipt requested, so you can document what the company received and when. Keep a file of your correspondence and enclosures.

If you're not certain that an account has been tampered with, but suspect that you may have provided information about it to the con men, then notify the institution with which the account is held in writing, and consider closing or suspending the account until you can be certain that there is no danger.

Getting Your Money Back

After you've alerted the credit reporting agencies and filed police reports, what next? Now you need to take a deep breath and prepare yourself for the challenges ahead. Don't expect this process to be easy – it won't be. Most victims later cite the psychological impact as being the most devastating consequence of the crime. It's important that you begin to discuss your experiences early in the process with trusted friends, family or a spiritual advisor.

Most people are determined to at least try to get their money back. If you decide to pursue this option, it's important that you seek advice from a fraud specialist, such as those at the Fraud Discovery Institute. You're unlikely to out-smart the bad guys on your own. Even when professionals are involved, recovering monies lost is rare.

In the past, we've been able to help a few victims recover their money by using some deception of our own – for instance, by leading the con men to believe that you (the victim) has a friend or relative with "real money" who is considering investing or purchasing in the scam.

After stringing them along with this hot prospect for awhile, you can attempt to try to persuade this high roller that the opportunity is legitimate by allowing you to "cash out" as a sign of good faith. Other victims have had success by asking to cash out of an investment in order to purchase a new home or some other large, temporary expense. The request is always made with the promise that the victim will return to the investment soon, perhaps with even more money to invest.

Trying to manipulate con men is not the work of amateurs and is usually best left to professionals in law enforcement or fraud prevention. Still, there is little to be lost by trying.

Fallout Shelter

By now, you've reported the crime, contacted credit reporting agencies, and attempted to get your money back. Unfortunately, the process is just beginning. Losses from fraud can have major impacts on things like retirement planning, college savings, etc. In order to move forward, it's necessary to face your losses head on.

A good accounting of your losses is necessary, followed by a realistic appraisal of how it will affect you, both now and in the future. For some, a $20,000 loss can be painful, for others, it may mean having to work an extra five years before retirement and a radical change of plans.

Meet with an accountant or other trusted financial advisor. You may need to consider restructuring your retirement investments to help compensate for the loss. For

example, if you're nearing retirement, you might need to shift a portion of your savings into investments that offer the potential for greater returns. (Remember that this will also mean higher risk, so it's important to consult your advisors.)

Taking care of yourself and your mental state is also important. Fraud is a crime, no more and no less than robbery or assault. And being a victim of fraud doesn't mean that you're stupid or gullible. It means that someone deliberately harmed you, through no fault of your own.

For many victims, participating in the pursuit of justice can help to bring a sense of closure. Follow up with the law enforcement agencies that you filed reports with, offer to testify at trial as needed, and provide any documentation that officials request. Many victims will seek other ways to help deal with the crime, such as getting involved in prevention efforts, seeking to have tougher laws enacted, or advising others who have been victims.

By taking these types of proactive steps, you can regain a sense of control and avoid more serious problems like depression. Resolve to be better informed and do more homework in the future, but don't allow the crime to turn you into a hermit. Any investment or opportunity also carries with it an amount of risk – without those risks, there would be no return. Don't allow your victimization to prevent you from taking risks in the future, but do let it teach you to be more cautious.

Remember, if you allow fear to control you, then the bad guys really do win. I've spent my life teaching people an important lesson: that "people can change." That includes the bad guys and the good guys. Both can grow and learn.

Lastly, when you've had some time to recover from your loss, I'd encourage you to consider one last action: forgiveness. It's difficult to even think about forgiving someone who has taken so much from us, especially if they don't seem concerned about the impact of their crimes. But holding on to that anger hurts you more than them... and likewise, forgiving them really helps you to close that chapter in your life.

Additional Resources For Victims of Fraud

Report fraud to all of the following government agencies:

A. Your State Attorney General's Office (Blue Pages in your phone book)
B. The Federal Bureau of Investigation (Blue Pages) ***www.fbi.gov***
C. The US Postal Inspection Service (Blue Pages) ***www.usps.com/postalinspectors***
D. The Federal Trade Commission (Blue Pages) ***www.ftc.gov***
E. The US Secret Service (Blue Pages) ***www.secretservice.gov***
F. Better Business Bureau (White Pages) ***www.bbb.org***
G. Your Local Police Department (White Pages)

Be Your Own Investigator

Résumés don't lie, but people do

The single biggest factor contributing to the growth of fraud since 1990 has been the use of the Internet by scam artists. They've found all kinds of inventive ways to use this telecommunications tool to further their schemes, but you can turn this weapon against them.

Using the Internet, you can play "private detective," and you'll be amazed at how much information you can gather. Let's look at some of these tools and how you might use them:

Commercial Search Services: There are dozens of businesses that will search computerized public records for a small fee. For most people, this is both the most practical and effective method of checking out a broker, business, or individual. You'll need to gather some basic facts: name, address and telephone numbers. Better yet, ask your broker for a résumé or biography. Most professionals have these and are happy to provide them. Just don't make the mistake of taking them at face value.

Some of the most established commercial record search companies are:

Intelius 425.974.6100 • ***www.intelius.com***

NetSleuth ***www.netsleuth.com***

There are many amateur detective sites that provide resources for performing background checks.

Do It Yourself Detective: If you're comfortable with doing research on the computer, and don't mind spending a few hours, you can learn nearly as much by doing the searches directly. There are some Web sites that offer tools to help speed up this process. For example, Yahoo offers a sleuth aid site at ***http://people.yahoo.com/.***

This single page allows you to search a person's name, do "reverse phone searches" in which you enter a phone number and it retrieves the billing information for that number, and even do address searches.

There are also many "amateur" detective sites that provide resources for people attempting to do their own background checks. For example, Richard Smith, a computer professional, maintains such a site at:

http://www.computerbytesman.com/sleuth/index.htm

or ***http://www.zabasearch.com/.***

Uncovering fraud, before it buries you.

When evaluating a company or investment offer, it's always a good idea to do individual background checks on the officers or board of directors. Often the company may appear to be legitimate, but a quick background check of the principals may reveal past legal troubles, pending criminal cases or SEC investigations. "Trust but verify" is the key when considering large investments or purchases.

When looking into publicly-held companies there are a variety of insightful sites that will provide filing notices, information on the board of directors, etc. Some of the best are ***http://10kwizard.ragingbull.com/*** and ***http://www.siliconinvestor.com/.***

Even simple techniques such as Google searches can tell you a lot about the person that you're considering doing business with. Take the time to learn some advanced search techniques to speed up your investigations. For example, say that you wanted to do a background check on Barry Minkow:

Go to: ***www.google.com***

Type in my name, but instead of doing it as usual, add quotation marks around the names, such as "Barry Minkow". You're simply telling the search engine that you only want to view pages where the name appears exactly as listed between the quotation marks.

Using even this simple technique quickly leads you to my personal Web site, and a ton of articles about my background, current projects, television appearances, etc. It would be a simple matter to verify everything that I've told you about myself.

In addition to checking out business opportunities, or investments, you can use these same tools to check up on people in critical jobs such as nannies or other caregivers. Remember, "Trust but verify."

Created by: Barry Minkow and John Broaddus

Executive Producer: Barry Minkow

Executive Producer: John Broaddus

Producer: Abby Rayburn

Writer: Wayne Franklin

Package Design: Dan Carpenter

Distributed by MDI Distribution