FRM-RHF.116

LET THE CONSUMER BEWARE IN TOUGH ECONOMIC TIMES

Consumer fraud is a continuing problem nationwide. In 2011, more than 1.8 million complaints were filed with various government agencies. This is a significant increase from 2010 when more than 1.4 million complaints were filed. That is an increase of 400,000 complaints in a single year.

Swindlers remain unendingly creative in their quest for newer and more ingenious scams. Scammers and rip-off artists come in all shapes, sizes, and colors. Don't think that you'll be able to recognize one by his or her looks. It's in their interest not to stand out. They can look ordinary and even respectable, and could even be prominent in the community, like Bernie Madoff. Or they could appear to be officials, with a badge or other fake credentials. And many fraudulent offers come from people you never even meet, via e-mail or the Internet.

People need to be wary not only of the signs of a swindler but also of the qualities within themselves that mark them as an easy victim. Do not assume that bad things only happen to the other guy. If you let down your guard, unscrupulous people can much more easily take advantage of you. It's true that people sometimes get lucky, but it's not often that you can get something for nothing. Try to look critically at any offer or "gift" that's too good to be true. When you do encounter such an offer, take some time to think things through. If the seller doesn't want to give you time to think before you commit your money, he or she probably is running a shady operation. The following information covers several of today's most pervasive types of frauds.

SURGE IN IDENTITY THEFT

For the ninth year in a row, identity theft was the No. 1 consumer complaint area; 26 percent of all consumer complaints were related to identity theft. And many instances of identity theft are perpetrated by someone the victim knows.

Credit card fraud was the most common form of reported identity theft, with 20 percent of complaints. Next were government documents / benefits fraud at 15 percent and employment fraud at 15 percent.

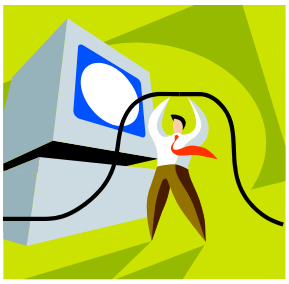
Some estimates say that one in five families is affected. Those committing such crimes include terrorists seeking false identities and funds for their acts of violence. They gain the information to steal identities through various means, some well within the control of potential victims.

Too many people are fooled into giving out their personal information, such as Social Security, credit card, or driver's license numbers, or their mother's maiden name, often to a total stranger who calls them by phone. If you do, you may find strange or unauthorized items charged on your credit card. Thieves often open new checking

accounts and credit cards in their victim's name and change the person's address to a vacant lot or a post office box. Most consumers don't find out that someone stole their identity until debt collectors start calling their home or they are turned down for credit. It may take them years to straighten out their finances and get back their good name.

If you find anything unusual on a bill, don't wait to see what happens next. Under the Fair Credit Billing Act (FCBA), you have the right to dispute any questionable charges made.

But you must file your dispute in writing. If fraud has taken place, notify local law enforcement, the Kentucky Attorney General's Office, and the Federal Trade Commission. (See contact information at the end of this publication.)



AVOID IDENTITY THEFT BY PROTECTING PERSONAL INFORMATION

Your Social Security number and mother's maiden name are usually needed to steal your identity. Among other information you should keep private are your driver's license and credit card numbers, as well as your birth date. When filling out forms or making a purchase, give only necessary information. Don't feel bad about leaving blanks if someone asks too much.

Experts recommend the following guidelines to avoid identity theft:

- Keep your Social Security card in a secure place, not in your wallet; and don't print the number on your checks.

- Keep your receipts for credit card purchases and thoroughly check every statement as soon as it comes in. Request your credit report from all three national credit bureaus every year.

- Don't leave personal information where someone may see it, and be sure to shred items that include personal information before you throw them away.

- Keep your mail secure, as thieves may steal *your* credit card offers or other sensitive information and apply for credit in your name. If necessary, get a post office box.

- Contact your bank, credit card company, and any other financial institutions, and "opt out" of having the company share your personal information.

- Remove your name from national mailing lists by contacting the Direct Marketing Association's Mail Preference Service. (See contact information at the end of this publication.)

- Stop financial institutions from sending you pre-approved offers of credit. (See contact information at the end of this publication.)

- Request that the three major credit bureaus put fraud alerts on your credit record if you have experienced any suspicious activity. Then they will be required to call you if any credit is requested in your name.

There are no laws prohibiting businesses or nonprofit organizations from asking for Social Security numbers; on the other hand, no law requires you to give your Social Security number to a business or organization. Many supermarkets and other stores, as well as libraries, will accept your telephone number or some other number instead, if you ask. However, you may need

to talk to the owner or manager directly if the clerk insists. And if you find stores or a local library that will not honor your request, and you belong to a local organization, club, or church, ask the president of your organization to send that business (or your mayor) a letter on behalf of the group, expressing the group's concern. Public pressure usually changes business or governmental practices such as these.

A comprehensive consumer guide, "What to Do if Your Personal Information Has Been Compromised," and other helpful resources are available from the Federal Trade Commission's Web site, http://www.ftc.gov/bcp/edu/microsites/idtheft/index.html, and also from the FTC's Consumer Response Center, 600 Pennsylvania Avenue, N.W., Washington, DC 20580; and by a toll-free call at (877) FTC-HELP (877-382-4357); TTY for the hearing impaired (866) 653-4261.

IDENTITY THEFT ON THE WORLD WIDE WEB

In a 2009 government report, of those who reported the method of initial contact, 52 percent said they were contacted by e-mail, and another 11 percent said an Internet Web site. Only 7 percent of those consumers reported the phone as the initial point of contact.

In today's high-tech world, your personal information could be almost anywhere without your knowledge. Businesses as well as governments collect people's personal information and store it in databases, and they don't have to tell you they're collecting yours. And just because the information is in a database doesn't mean it is safe. In January 2009, customer debit cards from Forcht Bank in Lexington, Kentucky, were compromised when another business's computer system was hacked. The security breach also affected customers of other banks and debit and ATM networks. *The security breach affected 8,500 consumers, and this is hardly an isolated case*.

IRS E-MAIL SCAM

Be wary if you receive an e-mail from someone claiming to be from the IRS, who notifies you of an "IRS e-audit." You might be asked to fill out a questionnaire – including Social Security number, bank account numbers, and other personal information – and given only 48 hours to complete the questionnaire to avoid penalties and interest. This type of scam also could be conducted by a stranger calling you on the telephone. Do not give out this information. The IRS does not conduct "e-audits" and does not notify taxpayers of audits by e-mail; they also do not ask for this type of confidential information. If you receive such an e-mail or telephone call, immediately notify the IRS office in your area.

INTERNET SERVICE PROVIDER E-MAIL SCAM

The Federal Trade Commission's Web site includes the following scam warning: "If you receive an e-mail request that appears to be from your Internet Service Provider (ISP) stating that your 'account information needs to be updated' or that 'the credit card you signed up with is invalid or expired and the information needs to be reentered to keep your account active,' do not respond without checking with your ISP first."
Remember: The person best able to protect you is you. And it is in your best interest to have your personal information in as few hands as possible.

INTERNET FRAUD AGAINST GOVERNMENT AGENCIES

The newest trend in Internet fraud victimizes government agencies, which ends up costing all of us in higher taxes and/or reduced services.

The *Washington Post* reported the 2009 cyber theft of $415,000 from Bullitt County, Kentucky. Criminals in Ukraine used a computer virus to infect Bullitt County's computers. They changed officials' passwords and used their access to approve transfers of money. They also recruited dozens of co-conspirators in the U.S. to receive money and transfer it out of the country. It is clear that deceptive methods were used to make recruits think they were doing legitimate work. One unlucky recruit ended up owing her bank nearly $9,000. It is clear from this case that you should not respond to job offers and/or business opportunities sent via e-mail, as you never know who the employer is or what they're up to. Do not even click on links in e-mails you are not expecting, as these could be attempts to infect your computer and/or steal your personal information.

CREDIT CARD FRAUD

As we have seen, credit card fraud is an integral part of identity theft. The cost of credit card fraud in the United States was over $45.5 million in 2008, according to the Federal Trade Commission; it peaked at over $50 million in 2007, but could rise again.

Even if you are not personally a victim, you still pay for credit card fraud in higher credit card finance charges and annual membership fees. Additionally, businesses raise the cost of goods and services to cover their losses from credit card fraud.

Stealing a credit card is not the only type of credit card fraud. Thieves can pick discarded receipts out of trash cans to obtain card numbers. Dishonest clerks sometimes make extra imprints of cards for personal use or to sell. You should always pay attention to what sales clerks do with your card and keep the receipts for tax purposes, specifically in case of an audit.

Another type of credit card fraud involves winning a contest. You might receive a call stating that you have won an automobile or some other fabulous prize. However, the scam artist says, it is necessary for you to provide your Social Security number to "verify that you are the actual winner." The deception usually continues with you being asked for your credit card number because you are required to pay taxes on the prize. In this scheme, the con artist will use your credit card number, along with the additional proof of your Social Security number, to purchase thousands of dollars worth of merchandise and services at your expense.

If someone phones you and says that you need to "provide the information now or I'm instructed to go to the alternate winner," warning bells should go off in your head. Any reputable promotional firm will give you 24 hours to check out the company. If they don't, it's usually a warning signal of fraud.

A third form of credit card fraud is simply a rip-off. You receive a call informing you that you have been selected in a "marketing program" for an unbelievably low-priced travel package or other product. You are requested to provide your credit card number. Frequently, what you receive is not as desirable as the promotion made it seem. As a result, you end up paying more for the product than it is really worth.

Don't give out your credit card number until you check with the Kentucky Attorney General's Consumer Protection Office. You should ask whether the company you're dealing with has unresolved complaints.

If your cards are lost or stolen, call the issuers immediately. Most have a toll-free number for reporting missing cards, and some provide 24-hour service. By law, you

are not responsible for any unauthorized charges made after the time you report the loss or theft. Make sure that you ask for the name(s) of the person(s) you talk with; make a note of the date, time and phone number for future reference; and file this information in a secure place.

According to the Fair Credit Billing Act, $50 is the maximum amount you can be held accountable for if your credit card is used without your authorization. This amount is per card. If you inform the company of the loss before any charges are made, then you are not responsible for any amount. It is important that you follow up your phone call to the credit card company with a letter sent by certified mail with receipt requested so that there is documentation of the fact that you notified them.

If you are not aware that your card is missing or that someone has used your card number without your authorization, you probably will notice the unauthorized charges on your next billing statement. Always be certain to check each statement for unauthorized charges and billing errors, even if your card isn't stolen. If you aren't careful, you may be billed twice for the same item or you might not receive credit for an item you returned.

You have 60 days from the day the bill is sent to notify the card issuer, in writing, about billing errors. For billing errors, federal law requires you to write the company, not just phone them. Many consumers make the mistake of not following up a phone call with a written complaint when reporting a billing error. Consumers also frequently send their letters to the credit company payment address, not the address the company provides for billing errors. This mistake slows the process of correcting the problem. After establishing that you have not authorized the charges, you still are only liable for the first $50, no matter how much was charged. The card issuing company is required to make these corrections within two billing cycles after receipt of notification that there is an error.

Be especially careful with debit cards, as the Electronic Fund Transfer Act, which is substantially different from the Fair Credit Billing Act, applies to them. Under this act, you must report the loss of your debit card within two business days after you realize it is missing; otherwise, your loss per debit card could be as high as $500. If you do not report the loss within sixty days of receiving your statement, you could incur unlimited loss from your checking account, savings account, line of credit established for overdrafts, and all other accounts associated with your debit card. For this reason you should check every statement to make sure someone is not using your debit card number and pin number without your permission. It also is best to keep your debit card account separate from any other account. If you have been a victim of credit fraud, see the end of this publication for more information on "Where to Go for Help."

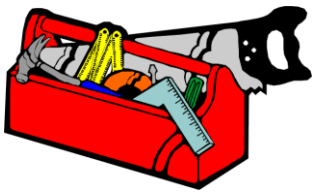
Credit cards have become an important part of the American economy. Some dishonest people, however, will try to use them to steal. Always treat your credit cards with caution. Be careful and alert. This will help you to avoid unnecessary costs and fees.

Free Annual Credit Report

The best way to get your free annual credit report is by going through the FTC-mandated Web site: AnnualCreditReport.com. The Federal Trade Commission, the nation's consumer protection agency, set up this Web site, where you can request a free credit report under federal law. This is due to a recent amendment to the U.S. Fair Credit Reporting Act, requiring each of the nationwide consumer reporting companies – Equifax,

Experian, and TransUnion – to provide you a free copy of your credit report, at your request, once every 12 months. Many other Web sites claim to offer "free" credit reports, but may charge you for another product if you accept a "free" report. Don't be fooled!

HOME REPAIR SCAMS



In 2008, the **homebuilding, repair and remodeling industry** resurfaced as the most inquired-about and complained-about industry at the Better Business Bureau of Central & Eastern Kentucky.

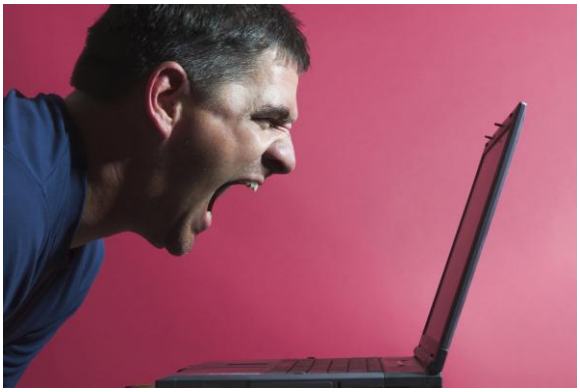
Home repair con artists usually work in older neighborhoods and prey on the elderly. Repair scams most often center on roofs or heating and cooling systems. Often the work is not necessary, although sometimes it is. If work really does need to be done, the scam artist will charge three to four times what it normally would cost.

Typically, a fly-by-night repairman comes to your door to say he "just happens to be in the neighborhood." He may claim to have just finished a paving job and offer to apply leftover asphalt to your driveway at a bargain price that turns out not to be a bargain. Sometimes these callers offer to spray coat the driveway with a sealer that turns out to be dirty car oil mixed with kerosene. This mixture will wash off with the next rain. Offers to paint barns may have the same result: the con artist uses watered-down paint or old oil and kerosene that wash right off.
Homeowners should not sign any contract without reading carefully to see what they are getting themselves into. It may be wise to have a competent lawyer read the contract first, before you sign. Even better, have the lawyer draft the contract for you, making sure the contract protects you from liability in case someone becomes injured on the job.

Some scam artists say they are "FEMA Certified," claiming approval by the Federal Emergency Management Agency. FEMA neither certifies nor endorses any private-sector contractor. Any contractor making such claims should be avoided. Also, poor workmanship is not a violation of Kentucky law; so be sure to hire an experienced, reputable contractor with good references and ask to see work that has been done before agreeing to anything.

Often consumers are left owing suppliers, even though they paid the contractor in full, not only for the work, but also for all materials used on the job. Don't let yourself be forced to pay twice for building supplies: Always pay directly to the suppliers for all materials.

Government officials caution homeowners to be very careful when hiring contractors to clean and repair disaster damage or to remove debris. Be wary when contractors predict disaster if the work is not done "today." Even for routine repairs and maintenance, check the contractors' references. Always get a second and third opinion and a couple of written estimates for any job. Get proof of insurance and ask for a written contract and a written guarantee. A good rule of thumb is never to hire a contractor whom you do not contact yourself. Never, under any circumstances, hire someone who knocks on your door. Pay by check, and have all work inspected.
Most likely, your home is the largest single lifetime investment you will make. Protect this investment by dealing with reputable and responsible businesses. It may seem expensive at the time, but not half as expensive as fly-by-night operators turn out to be. Remember, if it sounds too good to be true, it's probably not true.



Where to Go for Help

For general fraud complaints, contact:

Consumer Protection Division
Office of the Kentucky Attorney General
700 Capitol Avenue, Suite 118
Frankfort, KY 40601-3449
(888) 432-9257
(502) 696-5389 (Division Switchboard)
http://ag.ky.gov/consumer/

National Fraud Information Center
(800) 876-7060 (9:00 a.m. - 5:00 p.m. EST, Monday - Friday)
www.fraud.org

The Better Business Bureau
East of Frankfort, call (800) 866-6668
www.lexington.bbb.org
West of Frankfort, call (800) 388-2222
www.ky-in.bbb.org

For more information on the Fair Credit Billing Act and the Electronic Fund Transfer Act, go to the following Web site:
http://www.ftc.gov/bcp/conline/pubs/online/payments.htm

Consumers with questions or complaints about 900 numbers can contact:
The Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580
(202) 326-2222
www.consumer.gov
(877) IDTHEFT
(877) 438-4338
www.consumer.gov/idtheft
(The FTC maintains a "Consumer Sentinel" database on fraud complaints)

National Fraud Information Center /
National Consumers League
1701 K Street, NW, Suite 1200
Washington, DC 20006
(202) 835-3323
www.fraud.org

To remove your name from national mailing lists, register online free of charge, or send your name and address with a check or money order for $1 to:
Direct Marketing Association
Mail Preference Service
PO Box 643
Carmel, NY 10512
https://www.dmachoice.org/dma/member/regist.action

Remove your name from lists to receive pre-approved offers of credit:
One toll-free call, 1-888-5-OPT-OUT (1-888-567-8688), will tell all three major credit reporting agencies – Equifax, Experian, and Trans Union – to remove you from their lists. They will ask for your Social security Number to begin the process**.**

References

Better Business Bureau. (2009, February 17). “Top 10 List - Complaints and Inquiries” [Press Release]. Retrieved July 28, 2009, from http://www.bluegrass.bbb.org/NewsStory.asp?sid=090217Top10

Consumer Fraud Reporting. (n.d.). “FreeCreditReport.com Scam: FreeCreditReport.com is NOT the website to get your free annual credit report!” Retrieved July 28, 2009, from http://www.consumerfraudreporting.org/freecreditreportdotcom.php.

Federal Trade Commission. (2009, February). *Consumer Sentinel Network Data Book for January – December 2008*. Retrieved July 28, 2009, from http://www.ftc.gov/sentinel/reports/sentinel-annual-reports/sentinel-cy2008.pdf.

Federal Trade Commission. (2009, February 26). “FTC Releases List of Top Consumer Complaints in 2008” [Press Release]. Retrieved July 28, 2009, from http://www.ftc.gov/opa/2009/02/2008cmpts.shtm

Federal Trade Commission. (2012, February 28). FTC Releases Top Complaint Categories for 2011. [Press release]. Retrieved March 7, 2012, from http://ftc.gov/opa/2012/02/2011complaints.shtm.

Robert H. Flashman, Ph.D.
Extension Specialist in Family Resource Management

Alex Lesueur, Jr., M.S.L.S.
Staff Support Associate

September 2009; revised February 2011; March 2012