

# NEWSLETTER

July / August / September 2004

## Next Meeting of the Coalition

Wednesday, July 14, 2004  
8:30am – 11:00 am  
1st Floor Conference Mtg Rm  
455 Sherman Street  
Denver, CO

### Program: "Identity Theft"

*Program/Meeting is open to anyone who would like to attend. You do not need to be a member of CCERAP.*

### Guest Speakers:

Don Childears, President/CEO  
Colorado Bankers Association  
Rob Hendricks, Officer  
Tyson Kerr, Officer  
Sterling Police Department

### Meeting/Seminar Schedule:

8:30 – 9:00am  
Continental Breakfast  
9:00 – 9:30am - Seminars  
"Identity Theft Prevention  
Basics"  
"Identity Theft Through The Eyes  
of Law Enforcement"  
10:00 - 10:30am  
Questions & Answers  
10:30 - 11:00am Meeting  
Legislative Update  
POA Task Force Update  
Networking Spotlight -  
"Before the Money Is Gone"  
Adjournment

### Directions to Meeting:

Take I-25 to 6th Ave East  
Take 6th East to Broadway  
Take Broadway South to 4th  
Take 4th east to Sherman  
Building is on the corner of  
Sherman & 4th

### CCERAP Coordinator:

Kathy Rickart  
970-674-1774  
970-674-8712 fax  
Email: CCERAP@comcast.net

## Stealing Your Identity

By James P. Ruth, CFPN, Potomac Financial Group, Gaithersburg, MD  
Source: National Association of Retired Federal Employees Magazine, June 2004



Identity theft (IT) is one of the fastest growing crimes in America. The number of victims and dollar amounts stolen are staggering. According to the Federal Trade Commission (FTC), 9.9 million Americans were victims of some form of identity theft in 2002. Consumers and businesses lost over \$53 billion in these identity heists. While the media have given this type of crime a high profile in their coverage, most consumers have done little to protect themselves from being its next victim. IT at any age is a major disruption of your life. However, when you're retired, it can be even more devastating. While you are generally not liable for more than \$50 for credit card or bank fraud, you can spend months or even years reclaiming your good name and credit.

There are two distinct types of identity theft. The first is called "account takeover". Here the thief acquires your current credit card number and account information and then purchases goods and services for their personal use or to be later sold for cash. They may use your stolen credit card or be able to make the purchase just with your account number and the expiration date on your credit card. The second type, called "application fraud," is often more serious because the thief, armed with your Social Security number and other personal information, opens new accounts in your name. Then they go on a spending spree using your name and credit. You may not find out about the scam for months because the charge account bills go to an address established by the imposter.

While it is nearly impossible to prevent a committed thief from stealing your identity if they have singled you out, there are certain things you can do to make sure you are not a random victim. This list will help minimize the risk of being victimized.

- **Mail:** Most residential and rural mailboxes are not locked and provide juicy targets for thieves who easily steal both incoming and outgoing mail without even getting out of their car. Stop using an unlocked mailbox for outgoing mail. Deposit in a post office collection box. Better still; take your mail directly to the post office. If you must use an unlocked mailbox for incoming mail, make it a habit of picking it up promptly after delivery.
- **Credit Card and Credit Offers:** Keep all the receipts in an envelope or file folder each month in order of purchase. Then when your statement comes, you can easily check your receipts against the purchases. A few extra minutes a month here can help you nip a potential problem in the bud. Shred all unwanted offers of credit including the preprinted checks.
- **Trash:** Some thieves resort to stealing your garbage in order to steal your identity. Don't make it easy for these "dumpster divers" to steal your personal and financial trash. Always shred these documents before disposing of them.
- **Wallets and Purses:** Don't carry any more cards or identifying information than you need to conduct your daily business. At least once a year, photocopy everything in your wallet and keep it in a safe deposit box. It will be much easier to notify authorities.
- **Telephone Scam:** Often imposters will call you at home, posing as legitimate business or government officials for the purpose of securing personal identity information. Regardless of how legitimate the scheme sounds, NEVER give out personal information over the telephone.

- **Shoulder Surfing:** Looking over your shoulder at ATM machines and public telephones offers a perfect opportunity for thieves to lift your personal identification number (PIN). Shield possible viewing opportunities with your body or hands. Also, don't be bashful to ask a stranger to step back while you conduct your personal business.

Recognizing identity theft and taking a few simple measures should go a long way toward safeguarding your identity.

*James P. Ruth, CFP, is president of Potomac Financial Group and a registered representative offering securities through Mutual Service Corporation, member NASD/SIPC. His article is printed with his permission and the permission of NARFE Magazine, Margaret Carter, Director of Communications.*

Plan to attend the July 14, CCERAP meeting, to learn more about identity theft, what it is, how it effects the elderly, tips to share with the elderly to minimize their risk. Hear what one bank representative & two police officers have to say about identity theft and the challenges each face in regards to this crime. Details on meeting agenda, time and place on front page.

## Myth: The Elderly Don't Need to Worry About ID Theft

By Kathy Rickart, CCERAP Coordinator



Granted, when the elderly reach the "golden years" their home is usually paid for and they don't need to establish a good credit rating, so what's the hype all about? So what if they are victims of identity theft. They don't need to get a mortgage loan and many aren't worried about their credit rating any more. Plus you never heard of anyone losing money from identity theft. It's the credit card companies that lose the money. Big deal!

**WRONG!**

Read some of the victim reports sent to the Federal Trade Commission:

*"I have been denied auto insurance and medical insurance."*

*"I learned that someone had been working under my Social Security number for a number of years. He was arrested and used my SSN on his arrest sheet."*

*"About a year after my purse was stolen, I received information that someone using my identity had defaulted on a number of lease agreements and bought a car."*

*"Tomorrow is Sunday so we won't get any notices, but I'm not looking forward to Monday's mail."*

*"When I renewed my driver's license by mail, I was surprised to find someone else's face on my license. This is a nightmare..."*

*"I'm tired of the hours I've spent on the phone and all the faxing I've had to do. When will it be over?"*

It's not so much the elderly need the credit rating, as what they don't need when identity theft happens.

The elderly.. **DON'T NEED** – a criminal record to clear.

**DON'T NEED** – to spend leisure hours on the phone, investigating, faxing, etc.

**DON'T NEED** – to fear answering the phone as it might be another bill collector.

**DON'T NEED** – to lose sleep or their health due to worry, harassment or victimization shock.

**DON'T NEED** – the extra expense for certified mail, postage, copies, faxes, etc... It all adds up, so who says there's no money loss?

Some people have even had to hire lawyers.

**DON'T NEED** - the humiliation, anger and frustration as they try to reclaim their identity.

**AND - IT'S NOT ALL ABOUT LOSING MONEY!** Other things are at stake – for example, the way the elderly want to spend their time, their mental and physical health. If identity theft ruins their health, no amount of wealth will replace it! Just for that reason alone, the elderly should be concerned about ID Theft.

### ID Theft Educational Videos

Available from CCERAP for Loan

**Identity Theft –  
The Name of the Game**  
14 minutes



**Senior Security I –  
Avoiding Scams and Fraud  
in Colorado**  
29 minutes

Order using the change of information notification form on the back of the newsletter and check Video Order at the bottom of the form.

## Thank You

Colorado Division of Insurance and Senior Assistance Program for your continued sponsorship of the CCERAP Newsletter!

# Dealing with Collection Agencies – Some are Good, Some Are Awful!

By Kathy Rickart, ID Theft Victim

When the year 2000, marking the new Millennium rang in, so did the prediction “*ID Theft will be the crime of the century.*” Who pays attentions to those predictions anyway?

On December 15, 2000 we got a phone call from a credit card company asking my husband why he had not paid his bill. “*What bill? We don’t have that credit card.*” The lady on the other end of the line asked a few questions and it was obvious we were just enrolled in a crash course of “*ID Theft 101*” whether we liked it or not. She was extremely helpful and gave us information on the first steps we should take, like calling the credit bureaus. We seemed to be doing okay with just a few hitches here and there along the way, but then the nightmare of collection agencies began for those credit cards, taken out in my husband’s name, that we had not discovered yet.

The man from the collection agency on the other end of the line was admonishing me. He said it was my fault and that my children were probably using the credit card and I should stop trying to weasel my way out of paying the bill. I told him repeatedly we didn’t have that credit card and that we were victims of ID theft and this was probably another card taken out in our name. I asked him to read me the information on the application, as other credit cards taken out in my husbands name had a bogus mother’s maiden name and place of work. (*We’re retired.*) I pleaded with him to send me copies of the statements and the credit card application he kept referring to so I could verify the expenditures and application signatures. He said he didn’t have to prove anything - we were the guilty ones and needed to pay the bill. The discussion got heated and he had me in tears when I hung up the phone in anger. But that didn’t stop him; he called back and told me if I didn’t pay the bill, he would report us to the IRS. It wasn’t bad enough he had totally upset me, now he was threatening us! What was I going to do? Should I just pay it to save my sanity? No, we were not guilty of anything and I had enough German stubbornness in me - so I refused to give in.

Then someone gave me the booklet “*ID Theft-When Bad Things Happen to Your Good Name*”, first produced in February 2001 by the Federal Trade Commission. Although it was not in print when ID theft happened to us in the year 2000, I was ever so happy to have something that was of help in dealing with this crime. I had done the correct things, but not necessarily in the order that would have made it easier. There weren’t too many holes I still needed to address. As I read the booklet, about mid-way was the section – **DEBT COLLECTORS**. Just what I needed!

Let me share this section:

The Fair Debt Collection Practices Act prohibits debt collectors from using unfair or deceptive practices to collect overdue bills that a creditor has forwarded for collection.

You can stop a debt collector from contacting you by writing a letter to the collection agency telling them to stop. Once the debt collector receives your letter, the company may not contact you

again – with two exceptions: they can tell you there will be no further contact and they can tell you that the debt collector or the creditor intends to take some specific action.

A collector also may not contact you if, within 30 days after you receive the written notice, you send the collection agency a letter stating you do not owe the money. (*Note: I recommend you send the letter certified with a return card to document the letter was received, and always keep a copy.*)

Although your letter should stop the debt collector’s calls and dunning notices, it will not necessarily get rid of the debt itself, which may still turn up on your credit report.

A collector can renew collection activities if you’re sent proof of the debt. So, along with your letter stating you don’t owe the money; include copies of documentation that support your position.

If you’re a victim of identity theft, include a copy (NOT the original) of the police report. If you don’t have documentation to support your position, be as specific as possible about why the debt collector is mistaken.

The debt collector is responsible for sending you proof that you’re wrong. For example, if the debt in dispute originates from a credit card you never applied for, ask for the actual application containing the applicant’s signature. You can then prove that it’s not your signature on the application. In many cases, the debt collector will not send you any proof, but will instead return the debt to the creditor.

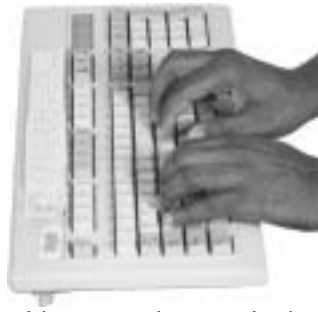
“*Bingo!*” I had done everything right on my end. I was still being harassed, so the next call I warned the debt collector that I was going to report them to the Consumer Affairs department in their state if he didn’t stop calling. The next call, I told him I was sending in a report, hung up and put my prepared letter with documentation in the mail to the Consumer Affairs Department. I never heard from the debt collector again, but did hear from the Consumer Affairs Department. The company was put on probation.

But it wasn’t over. January 2003 another collection agency called. I can’t tell you the “*fear in my heart*” thinking, “*Oh no, it’s starting over again.*” But it was in reference to the same credit card, just a different collection agency. The debt collector was very nice. I told him I had documentation. He said to send it. I did. They investigated and determined it to be fraud. Over? No, I’m afraid it will never be over. I consider ID Theft like having an incurable disease. It’s in remission now. But our name could be sold to some corrupt person in another state and it could happen again. Although, I hope not! We are already senior citizens and we don’t need to add 10 years to our age each time it happens or get heart stopping calls from collection agencies.

*Curtis and Kathy Rickart are victims of ID Theft. It began without their knowledge in October 2000, when a perpetrator obtained three pieces of information – name, birth date and social security number. The thief proceeded to go online and obtain a multitude of credit cards. Although it couldn’t be proven, the perpetrators obtained the information needed for identity theft when mail was delivered to their old address in New Mexico two years after they moved to Colorado. The case was closed on the last known credit card in January, 2003, over 2 years later. They feel they were the lucky ones as they have heard of stories far more damaging than theirs.*

# The Doors and Windows are Locked, but....

Source: Federal Trade Commission



You may be careful about locking your doors and windows and keeping your personal papers in a secure place. But, depending on what you use your personal computer for, an identity thief may not need to set foot in your house to steal your personal information, SSN's, financial records, tax returns, birth dates, and bank account numbers may be stored in your computer – a goldmine to an identity thief. The following tips can help you keep your computer and your personal information safe.

- Update your virus protection software regularly, or when a new virus alert is announced. Computer viruses can have a variety of damaging effects, including introducing program code that causes your computer to send out files or other stored information. Be on the alert for security repairs and patches that you can download from your operating system's website.
- Do not download files sent to you by strangers or click on hyperlinks from people you don't know. Opening a file could expose your system to a computer virus or a program that could hijack your modem.
- Use a firewall program especially if you use high-speed Internet connection like cable, DSL or T-1, which leaves your computer connected to the Internet 24 hours a day. The firewall program will allow you to stop uninvited guests from accessing your computer. Without it, hackers can take over your computer and access your personal information stored on it or use it to commit other crimes.

---

## Give Me A “Get Out of Jail” Card – QUICK!

Source: Federal Trade Commission

If you find yourself in a criminal situation due to identity theft, the following can be used as a guideline even though the criminal justice systems vary for state to state and even from county to county.

If wrongful criminal violations are attributed to your name:

- Contact the police or sheriff's department that originally arrested the person using your identity, or the court agency that issued the warrant for arrest.
- File an impersonation report and have your identity confirmed using your identification documents, i.e.: driver's license, passport or visa. Ask that these documents be compared with those of the imposter to establish your innocence. If not in the state you reside, ask your local police department to send the impersonation report to the jurisdiction where the criminal action originated.
- When you get a clearance letter or certificate of release (if you

- Use a secure browser –software that encrypts or scrambles information you send over the Internet – to guard the security of your online transactions. Be sure your browser has the most up-to-date encryption capabilities by using the latest version available from the manufacturer. You can also download some browsers for free over the Internet. When submitting information, look for the “lock” icon on the browser's status bar to be sure your information is secure during transmission
- Try not to store financial information on your laptop unless absolutely necessary. If you do, use a strong password – a combination of letters (upper and lower case), numbers and symbols. Don't use an automatic login feature, which saves your user name and password so you don't have to enter them each time you login or enter a site. And always log off when you're finished. That way, if your laptop is stolen, it's harder for the thief to access your personal information.
- Before you dispose of a computer, delete personal information. Deleting files using the keyboard or mouse commands may not be enough because the files may stay on the computer's hard drive, where they may be easily retrieved. Use a “wipe” utility program to overwrite the entire hard drive. It makes the files unrecoverable. For more information, see *Clearing Information From Your Computer's Hard Drive*, ([www.hq.nasa.gov/office/iog/hq/hard\\_drive.pdf](http://www.hq.nasa.gov/office/iog/hq/hard_drive.pdf)) from the National Aeronautics and Space Administration (NASA).
- Look for website privacy policies. They answer questions about maintaining accuracy, access, security, and control of personal information collected by the site, as well as how information will be used, and whether it will be provided to third parties. If you don't see a privacy policy, consider surfing elsewhere.

---


were arrested), KEEP this document with you at ALL times, in case you are wrongfully arrested.

- Ask the law enforcement agency to file, with the district attorney's (D.A.) office and/or court where the crime took place, the record of the follow-up investigation establishing your innocence. This will result in an amended complaint being issued. Once your name is recorded in the database, it's unlikely that it will be completely removed from the official record. Ask that the “key name,” or “primary name” be changed from your name to the imposter's name (or to John Doe if the imposter's true identity is not known), with your name noted only as an alias.
- To clear your name in the court records, contact the D.A.'s office in the county where the case was originally prosecuted. Ask the D.A.'s office for the appropriate court records needed to clear your name.
- Finally, contact your DMV to find out if your driver's license is being used by the identity thief. Ask that your files be flagged for possible fraud.

You might need or want the help of a criminal defense attorney to help you clear your name. If so, contact Legal Services in your state or your local bar association for help in finding an attorney.

# Social Security Numbers Source: Federal Trade Commission

Financial institutions and employers will likely need your SSN for tax reporting and wage purposes. Other businesses may ask you for your SSN to do a credit check, like when you apply for a loan, rent housing, or sign up for utilities. Sometimes, however, they simply want your SSN for general record keeping. You don't have to give a business your SSN just because they ask for it. Sometimes your SSN is required when submitting information for a picture ID card you must wear or present. If you see that your SSN is going to be on the card you wear around your neck and thus visible to everyone, ask them to remove it or blot it out.

It seems like every one asks or every form you fill out:  If someone asks for your SSN, ask the following questions:

- ? – Why do you need my SSN?
- ? – How will my SSN be used?
- ? – What law requires me to give you my SSN?
- ? – What will happen if I don't give you my SSN?

Name: _____
Address: _____
Phone: _____
Social Security Number: _____

Sometimes a business may not provide you with the service or benefit you're seeking if you don't provide your SSN. Getting answers to these questions will help you decide whether you want to share your SSN with the business. Remember the decision is yours.

But if identity theft happens and you are certain the thief is using your SSN, should you apply for a new social security number?

Under certain circumstances, SSA may issue you a new SSN – at your request – if:

- After trying to resolve the problems brought on by identity theft, you continue to experience problems.

Consider this option carefully:

- A new SSN may not resolve your identity theft problems, and may actually create new problems. For example, a new SSN does not necessarily ensure a new credit record because credit bureaus may combine the credit records from your old SSN with those from your new SSN.
- Even when the old credit information is not associated with your new SSN, the absence of any credit history under your new SSN may make it more difficult for you to get credit.
- And finally, there's no guarantee that an identity thief would not misuse a new SSN.

A final word about Social Security Numbers – **DO NOT CARRY YOUR SOCIAL SECURITY CARD IN YOUR WALLET OR PURSE!** The same goes for Medicare Cards since they have your SSN on them. Carry your Medicare Card only when you need it. If it is an emergency, they shouldn't deny you treatment if you don't have your card with you. It can be submitted later. Most Medical facilities that you usually use will have it on record.

---

## Tips on Filing a Police

### Report Source: Federal Trade Commission

#### 3 Provide Documentation

Furnish as much documentation as you can to prove your case. Debt collection letters, credit reports, your notarized ID Theft Affidavit, and other evidence of fraudulent activity can help the police file a complete report.

Note: You can go to [www.consumer.gov/idtheft](http://www.consumer.gov/idtheft) or contact CCERAP at [ccerap@comcast.net](mailto:ccerap@comcast.net) for a copy of the ID Theft Affidavit. It should be used to report any new accounts opened in your name without authorization or when unauthorized charge have been made on your account.

#### 3 Be Persistent.

Local authorities may tell you that they can't take a report. Stress the importance of a police report; many creditors require one to resolve your dispute. Also remind them that under their voluntary "Police Report Initiative," credit

bureaus will automatically block the fraudulent accounts and bad debts from appearing on your credit report, but only if you can give them a copy of the police report. If you can't get the local police to take a report, try your county police. If that doesn't work, try your state police. If you're told that identity theft is not a crime under your state law, ask to file a Miscellaneous Incident Report instead.

#### 3 Be a Motivating Force.

Ask your police department to search the FTC's Consumer Sentinel database for other complaints in your community. You may not be the first or only victim of this identity thief. If there is a pattern of cases, local authorities may give your case more consideration.

#### 3 File your complaint with the FTC.

[www.consumer.gov/idtheft](http://www.consumer.gov/idtheft)

If you haven't already filed a complaint with the FTC – do so. Law enforcement agencies use complaints filed with the FTC to aggregate cases, spot patterns, and track growth in identity theft. This information can then be used to improve investigations and victim assistance.

# Document, Document, Document And....Organize, Organize, Organize

Source: Federal Trade Commission

Accurate and complete records will greatly improve your chances of resolving your identity theft case.

- Follow-up in writing with all contacts you've made on the phone, in person or by mail. Use certified mail, return receipt requested.
- Keep copies of all correspondence or forms you send.
- Write down the name of anyone you talk to, what he or she told you, and the date the conversation occurred.
- Keep the originals of supporting documentation, like police records, and letters to and from creditors; **send copies only**.
- Set up a filing system for easy access to paperwork.
- Keep old files even if you believe your case is closed. One of the most difficult and annoying aspects of identity theft is that errors can reappear on your credit reports or your information can be re-circulated. Should this happen, you'll be glad you kept your files.

---

## Hot Off the Press – Social Security ID Alert!!

By Steve Potter, Public Affairs Specialist, Social Security Administration

We have recently received reports that members of the public have received calls from individuals who **allege to be calling on behalf of the Social Security Administration (SSA)**. The callers are asking for personal information such as their Social Security Number (SSN) and bank information.

- **If you receive such a call, take these steps.**

You should **never provide your SSN or other personal information over the phone**, unless you initiated the contact or are confident about who you are talking to (e.g., you are familiar with the name from previous contact with SSA.) SSA does not routinely contact beneficiaries by phone to obtain personal information.

Please contact the Office of Inspector General (OIG) Hotline to report the incident. See insert on "Identity Theft Resource List" for the SSA Fraud Hotline and other contact information.

### Procedure For Writing To The Hotline

If a caller chooses to send a written message to the hotline (i.e., via mail, FAX, or Internet), include the following information:

- name, address, phone number, and SSN of the alleged violator. If the SSN is unknown, include as much identifying information as possible (e.g., date of birth, place of birth, parent's names)
- complete description of the potential violation
- caller's name, address and phone number

NOTE: The caller's name is very important to an investigation and without it, SSA OIG may not be able to investigate the allegation.

---

## Nuts and Bolts on Selecting A Medicare Discount Card

By Robert Pierce, Colorado Division of Insurance,  
Senior Assistance Program

Coloradans on Medicare can save money on prescriptions with the new Medicare-approved drug cards, but confusion is keeping some consumers from signing up. Coloradans have more than 40 Medicare-approved drug card choices, but can only choose one of the cards.

The "Access to Benefits Coalition-Colorado" is providing assistance to Medicare consumers to make these choices. Coloradans can call 1-800-503-5190 and be connected to local help organizations across the state.

"We know that which card a consumer picks really makes a difference price-wise. For example, Prilosec 20 mg was priced as low as \$106 and as high as \$144 under the various drug cards. We'll help consumers find those drug cards that consistently provide lower costs," said Linda Whittington on behalf of ABC-CO.

ABC-CO is also concerned that those who qualify for a \$600 drug credit in 2004 apply for that new Medicare help. Any Medicare recipient who does not have drug insurance from a former employer or Medicaid and who meets income guidelines qualifies. Couples must have income of \$16,862 or less, and singles \$12,569 or less.

"The \$600 credit is very easy to apply for. The application form is short, assets like your investments and home are not considered, and you don't have to send in tax forms or other proof of income," Whittington said. "And those who qualify will automatically receive a second \$600 drug credit in 2005."

Medicare operates a website [www.medicare.gov](http://www.medicare.gov) where consumers can list their zip code and the drugs they take, and then generate a customized list of their drug prices through the various cards at local participating pharmacies. They call also call 1-800-Medicare and request the computer list. The 1-800-Medicare line operates 24 hours per day, 7 days per week, and callers are advised to contact them outside normal business hours to have shorter wait times.

# Identity Theft Laws – Have We Got Any In Colorado?

By Kathy Rickart, CCERAP Coordinator

When the Federal Trade Commission reprinted their updated booklet in September 2002 on ID Theft only Colorado, Hawaii, Maine, Nebraska, New York, and The U.S. Virgin Islands didn't have laws addressing identity theft. By end of 2003, Colorado was one of two states still without laws.

The 2004 Colorado Legislature is applauded for beginning to change the shameful status that put Colorado among the states with the most reports of identity theft. We now have two laws on the books that address identity theft. They are House Bills 1274 and 1134. The Governor signed House Bill 1127 in April and House Bill 1134 was sent to the Governor for signature at press time of this newsletter. Both go into effect July 1, 2004.

## Identity Theft Definitions:

**Biometric Data:** any data, such as fingerprints, voiceprints, or retina and iris prints that capture, represent, or enable the reproduction of the unique physical attributes of an individual.

**Identifying Information:** information that, alone or in conjunction with other information, identifies an individual, including, but not limited to: name, address, birth date, telephone, social security, taxpayer identification, driver's license, identification card, alien registration, government passport, or checking, savings, or deposit account number, biometric data, unique electronic identification devise or telecommunication identifying devise.

**Telecommunication identifying devise:** a number, code, or magnet or electronic devise that enables the holder to use telecommunications technology to access an account; obtain money, goods, or services; or transfer funds.

**House Bill 1274 Concerning: Identity Theft Section 1, Title 5, Colorado Revised Statutes, ARTICLE 3.7 – 5-3.7-**



## 101. Consumer credit solicitation protection

In a nutshell, this law describes the responsibilities of mail solicitation for credit cards by lenders. Basically it states the solicitor MUST verify the consumer accepting the mail solicitation is the same consumer to whom the solicitation was sent.

## Section 2, Title 13, Colorado Revised Statutes, ARTICLE 12 – 13-21-122. Civil liability for unlawful use of personal identifying information

A person who suffers damages as a result of an identity theft crime shall have a private civil right of action against the perpetrator who committed the crime, regardless of whether the perpetrator was convicted of the crime. The plaintiff shall be entitled to actual damages, including, but not limited to damage of reputation or credit rating, punitive damages and attorney fees and costs.

**House Bill 1134 Concerning:** The administration of programs relating to the prohibition against using identity information for unlawful purposes.

## Section 1, Title 42, Colorado Revised Statutes, ARTICLE 1 – 42-1-222. Motor vehicle investigations unit

The creation of a motor vehicle investigations unit to investigate and prevent fraud by using driver's licenses, identification cards, motor vehicle titles and registrations and any other vehicle documents issued by the motor vehicle department. This investigation unit will also be responsible for assisting victims of identity theft with documentation.

## Section 2, Title 16, Colorado Revised Statutes, ARTICLE 5 – 16-5-103. Identity theft victims

In a nutshell, this law gives the identity theft victim the opportunity for legal assistance in determining their innocence. If the victim is found innocent, they can obtain a court order certifying this determination. It allows the person who knows or reasonably suspects they are a victim of

identity theft to initiate a law enforcement investigation by contacting the local law enforcement agency that has jurisdiction over the victim's residence or over the place where a crime was committed. Furthermore, this law requires the law enforcement agency to take a police report, provide the victim with a copy of the report and begin an investigation of the facts. If the crime was committed in a different jurisdiction, the local law enforcement agency may refer the matter to the local law enforcement agency where the suspected crime was committed for investigation of the facts. If at any time, the facts bear the victimization to be false, the court order can be rescinded.

**House Bill 1122,** All identity theft was left with the House Committee on Appropriations and indefinitely postponed. Hopefully this bill will go forward in the future as it addresses even further the rights of the victim, thoroughly describes the identity theft perpetrator, and makes identity theft a crime under the "Colorado Organized Crime Act." It would make identity theft a class 4 felony. It also would expand criminal possession of a forgery devise to include defined written instruments, such as wills, deeds, contracts, promissory notes, etc. that are used for the purpose to defraud. This bill is by far the most complicated, but it is the only one that addresses the criminal act in regards to the perpetrator.

To get Colorado off the list of states with the most identity theft crimes, we need to make it unattractive to the perpetrator of these crimes. They need to suffer some consequences for their actions. It's not enough to stop at asking law enforcement to investigate to just prove the victims innocence. We need to give law enforcement the teeth needed to arrest and prosecutors a means to enact the law.

Copies of the new laws will be shared at the July 14, 2004 CCERAP meeting or you can download a copy by going to [www.leg.state.co.us](http://www.leg.state.co.us) and clicking Bills under House – Current Regular Session. Then do a search for the range the bill falls in. Find the bill number and click on the history to check its status in legislative action or click the download with the most current date for a copy of the bill.

# - IDENTITY THEFT RESOURCE LIST -

## CREDIT BUREAUS:

### EQUIFAX – [www.equifax.com](http://www.equifax.com)

To order your credit report: 1-800-685-1111  
To report fraud: 800-525-6285 or TDD 800-255-0056  
Write to: PO Box 740241, Atlanta, GA 30374-0241  
To get off credit card solicitation lists write:  
Equifax, Inc. Options  
PO Box 740123, Atlanta, GA 30374-0123

### EXPERIAN – [www.experian.com](http://www.experian.com)

For credit report or to report fraud: 1-888-397-3742 or  
TDD 1-800-972-0322  
Write to: PO Box 9532, Allen, TX 75013  
To get off credit card solicitation lists write:  
Experian Consumer Opt-Out  
701 Experian Parkway, Allen, TX 75013

### TRANSUNION – [www.transunion.com](http://www.transunion.com)

To order your credit report: 1-800-888-4213  
To report fraud: 1-800-680-7289 or  
TDD 1- 877-553-7803  
Fax: 714-447-6034  
E-mail: [fvad@transunion.com](mailto:fvad@transunion.com)  
Write to: TransUnion Fraud Victim Assistance Dept.  
PO Box 6790, Fullerton, CA 92634-6790  
To get off credit card solicitation lists write:  
TransUnion Marketing List Opt Out  
PO Box 97328, Jackson, MS 39288-7328

If you are reporting fraud, you only need to contact one of the credit bureaus. They are required by Federal Law to notify the others.

### To STOP Direct Mail Marketing:

Write: Direct Marketing Association,  
Mail Preference Service  
PO Box 643, Carmel, NY 10512  
*(Tell them you want your name placed on the "delete" file.*

On-line: [www.thedma.org/consumers/offmailinglist.html](http://www.thedma.org/consumers/offmailinglist.html)

### To STOP Telemarketing calls:

Write: Direct Marketing Association,  
Telephone Preference Service  
PO Box 1559, Carmel, NY 10512  
Or Sign up on the Colorado Do Not Call List by  
calling: 1-888-249-9097  
Or go register on-line at: [www.coloradonocall.com](http://www.coloradonocall.com)

### To REDUCE Unsolicited Commercial E-mail:

On-line: [www.dmaconsumers.org/offemalilist.html](http://www.dmaconsumers.org/offemalilist.html)  
*(This is effective for one year.)*

### ADDITIONAL GOVERNMENT BLUE PAGES (TELEPHONE BOOK) RESOURCES:

FEDERAL BUREAU OF INVESTIGATION (FBI) [www.fbi.gov](http://www.fbi.gov)  
U.S. SECRET SERVICE (USSS) [www.treas.gov/uss](http://www.treas.gov/uss)

## ATM OR DEBIT CARD: *(lost or stolen)*

Cancel the card. Get a new card with a new PIN.  
*(Report within 2 days, loss limited to \$50. Report between 3-60 days, \$500 limit. After 60 days, maybe all money taken will be lost.)*

## BANK FRAUD:

*If you are having trouble getting help to resolve banking related ID theft problems, go to [www.ffiec.gov/enforcement.htm](http://www.ffiec.gov/enforcement.htm) to discover which agency listed below has jurisdiction over your financial institution.*

### FEDERAL DEPOSIT INSURANCE CORPORATION (FDIC)

*(non members of Federal Reserve System) [www.fdic.gov](http://www.fdic.gov)*

Call: Consumer Call Center, 1-800-934-3342

Write: Federal Deposit Insurance Corporation, Division of Compliance and Consumer Affairs, 550, 17th Street, NW, Washington, DC 20429.

### FEDERAL RESERVE SYSTEM (Fed)

*(members of Federal Reserve System)*

[www.federalreserve.gov](http://www.federalreserve.gov)

Call: 202-452-3693

Write: Division of Consumer and Community Affairs, Mail Stop 801, Federal Reserve Board, Washington, DC 20551 or contact Federal Reserve Bank in your area.

### NATIONAL CREDIT UNION ADMINISTRATION (NCUA)

*(all federal and many state credit unions)*

[www.ncua.gov](http://www.ncua.gov)

Call: 703-518-6360

Write: Compliance Officer, National Credit Union Administration, 1775 Duke Street, Alexandria, VA 22314

### OFFICE OF COMPTROLLER OF THE CURRENCY (OCC)

*(all banks where "national" or the initials N.A. appear in the name)*

[www.occ.treas.gov](http://www.occ.treas.gov)

Call: 1-800-613-6743

Fax: 713-336-4301

Write: Customer Assistance Group, 1301 McKinney St, Suite 3710, Houston, TX 77010

### OFFICE OF THRIFT SUPERVISION (OTS) *(all federal and many state thrift, savings and savings and loan)*

[www.ots.treas.gov](http://www.ots.treas.gov)

Call: 202-906-6000

Write: Office of Thrift Supervision, 1700 G Street, NW, Washington, DC 20552

## BANKRUPTCY FRAUD:

*(someone has filed bankruptcy in your name)*

### U.S. TRUSTEE (UST) - DEPARTMENT OF JUSTICE (DOJ)

[www.usdoj.gov/ust](http://www.usdoj.gov/ust)

To Write: check the Blue Pages in your phone book under U.S. Government Bankruptcy Administration.

# - IDENTITY THEFT RESOURCE LIST -

## CHECKS: *(stolen or lost)*

Notify the bank. Stop payment and ask bank to notify the check verification service. If you fail to notify the bank, it is possible you will be held responsible for losses from a forged check. To find out if an identity thief has been passing bad checks in your name call:  
SCAN: 1-800-262-7771. Follow up all calls in writing. Certified with return card. Keep copies of your files. Make a police report with the local police. Get a copy of the police report.

## INVESTMENT FRAUD:

Immediately report it to your broker or account manager and to the SEC.

U.S. SECURITIES AND EXCHANGE COMMISSION (SEC)  
*(mishandling or tampering of investments)*

[www.sec.gov/complaint.shtml](http://www.sec.gov/complaint.shtml)

General questions, call: 202-942-7040

Write: SEC Office of Investor Education and Assistance, 450 Fifth St, NW, Washington DC, 20549-0213

## MAIL THEFT:

*(stolen mail by identity thief)*

U.S. POSTAL INSPECTION SERVICE (USPIS)

[www.usps.gov/websites/depart/inspect](http://www.usps.gov/websites/depart/inspect)

Report to your local postal inspector: Locate postal inspector by going to website above or calling your local post office.

## PASSPORT FRAUD:

*(lost or stolen passport being used fraudulently)*

UNITED STATE DEPARTMENT OF STATE (USDS)

[www.travel.state.gov/passport\\_services.html](http://www.travel.state.gov/passport_services.html)

Report using website or call a local USDS Office through the Blue Pages of your telephone directory.

## PHONE FRAUD:

*(unauthorized phone service established in your name or unauthorized calls are being made)*

LOCAL SERVICE: Contact your state Public Utilities Commission

CELLULAR AND LONG DISTANCE: Contact the Federal Communications Commission (FCC)

[www.fcc.gov](http://www.fcc.gov)

Call: 1-888-CALL-FCC, TTY: 1-888-TELL-FCC

Write: Federal Communications Commission, Consumer Information Bureau, 445 12th Street, SW, Room 5A863, Washington, DC 20554

E-mail questions: [fccinfo@fcc.gov](mailto:fccinfo@fcc.gov)

## SOCIAL SECURITY NUMBER THEFT & MISUSE:

SOCIAL SECURITY ADMINISTRATION (SSA)

[www.ssa.gov](http://www.ssa.gov)

Call: 1-800-269-0271

Fax: 410-597-0118

Write: SSA Fraud Hotline, PO Box 17768, Baltimore, MD 21235

E-Mail: [oig.hotline@ssa.gov](mailto:oig.hotline@ssa.gov)

To verify accuracy of earnings or to request a copy of your SS Statement call and follow-up I writing:  
1-800-772-1213

## TAX FRAUD:

INTERNAL REVENUE SERVICE (IRS)

[www.treas.gov/irs/ci](http://www.treas.gov/irs/ci)

Call: 1-800-829-0433

Having trouble filing tax returns due to ID theft call:  
IRS Taxpayer Advocates Office – 1-877-777-4778

## The booklet “ID Theft – When Bad Things Happen to Your Good Name”

produced by the Federal Trade Commission is probably the one and most complete booklets of information all forms of identity theft – including credit card fraud, mail fraud, wrongful arrest, etc.

Every article in this newsletter that lists Federal Trade Commission as the source was taken from this booklet and printed with permission from the FTC. Single copies are available by calling toll-free 1-877-438-4338. After talking to a representative recently about obtaining the booklet in bulk, it was noted the supply the FTC printed in September 2002, that was supposed to last 5 years, is depleted so you might need to go to:

[www.consumer.gov/idtheft](http://www.consumer.gov/idtheft) or to <http://www.fdic.gov/quicklinks/consumers/idtheft.htm>. You can download it from the first website. It is very, very long, so you might just want to put it in your “favorites” on your computer for easy reference.

## ID Theft Victims Take Action Now:

1. Contact the fraud department of any one of the three major credit bureaus to place a fraud alert on your file.
2. Close the accounts that you know or believe have been tampered with or opened fraudulently. Use the ID Theft Affidavit ([www.consumer.gov/idtheft](http://www.consumer.gov/idtheft)) when disputing new unauthorized accounts.
3. File a police report where you live. Get a copy of the report.
4. Follow-up in writing to #1 & #2 attaching a copy of the police report and other documentation you may have.
5. File your complaint with FTC.
6. Contact any of the other agencies specific to your particular type of ID Theft and follow-up in writing.
7. Document everything.

For additional help the Colorado Attorney General's Office has a website with an excellent guide.

Go to [www.ago.state.co.us/idtheft/victim.htm](http://www.ago.state.co.us/idtheft/victim.htm)