Identity Theft

KOFE

Knowledge of Financial Education

A product of CONSOLIDATED CREDIT™
When debt is the problem, we are the solution.

www.kofetime.com

Some Facts about Identity Theft:

- 30.8 million Americans have been victims of identity theft in the last three years, including 11.6 million people in the last year alone.
- Nearly 85% of all victims find out about their identity theft case in a negative manner. Only 15% of victims find out due to a proactive action taken by a business.
- 21% say it was a friend, relative or co-worker who stole their identity.
- The average time spent by victims trying to resolve identity theft issues is about 600 hours, an increase of more than 300% over previous studies.
- Last year's identity theft losses to businesses and financial institutions totaled $47.6 billion and consumer victims reported $5 billion in out-of-pocket expenses.
- Because this crime is often misclassified, the thieves have just a one in 700 chance of being caught by the federal authorities.
- The emotional impact of identity theft has been found to parallel that of victims of violent crime.
- Roughly half of all adults feel they do not know how to protect themselves against identity theft.
- Children are increasingly becoming victims of identity theft, according to the Identity Theft Resource Center.

How You Can Help Protect Yourself From Identity Theft

Unfortunately, there is no surefire way to protect yourself from identity theft. But there are steps you can take to minimize the chances that your information will be stolen and used by a thief. The first part of this publication is organized into checklists you can use to put these ideas into practice. The second part of this booklet will give you steps to take if you are a victim.

Keep It To Yourself: The less information that's out there,The better!

- **Carry only the cards** you need in your wallet. It's a good idea to leave extra credit cards and your Social Security card locked up safely at home.
- **Make a copy** of all your credit cards, front and back, and keep that list in a safe (locked) place in case your wallet or purse is stolen.
- **If your medical insurance card** lists your social security number, ask your insurance provider if you can change it to another number. If not, carry the card only when you need it for doctor's appointments etc.
- **If your driver's license number** is your social security number, ask your state if you can choose another number. Many states are starting to allow this.
- **When shopping,** take your credit card receipts with you and then store them in a safe place at home. Pay attention while your purchases are being rung up to make sure the card information isn't written down or copied an extra time.
- **Don't let a store clerk write your credit card number** or any unnecessary identification information on your check. If she wants to write down your driver's license number, for example, ask her not to write down the complete number. Ask to speak to a manager if the clerk insists on copying all your information onto your check.
- **Don't print your driver's license** or social security number on your checks.
- **When asked for your social security number,** always ask if you can provide another number. The more consumers insist on this, the sooner businesses will have to change their policies.
- **Don't use ATM machines** from financial institutions you don't recognize. Thieves have used ATMs to gather information from customers about their cards or accounts.

At Work: Don't let an ID thief catch you sleeping on the job.

- **Keep your purse locked up at work**. Workplace theft is more rampant than most people realize. Ask your employer for a safe place to lock your purse or wallet if none is provided.
- **Ask your employer about its security procedures** for personnel files. Make sure they are locked and that there is a policy in place to protect theft. Many cases of identity theft have originated at work, and involved coworkers stealing personal data.
- **Don't log onto personal financial accounts from work** and don't set work computers to remember personal passwords automatically. Finally, don't store personal information in your desk or in work computers.

At Home: Make sure your home is a safe haven.

- **Thieves can pluck bills** or other mail from your mailbox and use that information to commit fraud. To protect yourself, use a locked mailbox if possible to receive mail. (Type "locked mailbox" in an Internet search engine for sources.) Send any sensitive mail from the Post Office or using an official USPS mailbox.
- **Never have new checks sent to your home**, unless your mailbox is secure. Ask them to be delivered to your bank and pick them up instead.
- **Buy an inexpensive shredder** to shred any mail or documents with sensitive information.
- **Keep track of when your credit card bills normally arrive.** If one is missing, contact your lender immediately. Don't just assume you get to skip a month's payment!
- **Check your credit report** at least once a year (see How the New Credit Reporting Law Can Help You later in this booklet for more details). Consider a credit monitoring service if you want to keep close tabs on your credit report. Early detection of fraud can save hours of time and hassle later.
- **Each year,** you'll get your benefits statement from the Social Security Administration. Check it carefully for errors as well as possible fraud.
- **Keep your personal information** in a locked room or filing cabinet at home. This is especially important if you have frequent visitors (including your children's teenage friends), a housekeeper, or others who may be in your home.

Get Off the List: Protect your information and save a few trees.

- **Stop unsolicited credit card offers** by blocking your name from prescreening by the credit bureaus. Call 888-5OPT-OUT and all three major credit reporting agencies will be notified that you don't want to receive these offers.
- **End telemarketing calls** by signing up for the Federal Trade Commission's National Do Not Call Registry. National Do Not Call Registry, www.donotcall.gov, (888) 382-1222. You may want to register for your state's Do Not Call registry if available.
- **Consider an unlisted phone number,** or at least ask the phone company to list your name in the phone book with only an initial and no address.

- Opt-out of letting companies share your information. You should get annual privacy notices from financial institutions you do business with. Take a minute to read them and say no if you don't want them to share your information. There will be instructions for "opting out."

Safer Surfing: If you're not careful, your computer can be like an unlocked door into your home.

- **Use a firewall on your home computer.** These are often inexpensive, and well worth it. If you are connected all the time to the Internet via a cable modem or DSL, it's especially important to be protected.
- **Block your phone number** from reverse directories such as Anywho.com (www.anywho.com/help/privacy_list.html) and US Search (used on Yahoo: www.ussearch.com/wlcs/commerce/about/privacy.jsp).
- **Choose good passwords.** Don't use your social security number, address, dates of you or your children's birth, etc. The best passwords use letters and numbers, but don't be obvious (your child's name and date of birth, for example).
- **Watch user names, too.** Don't use email addresses or user names that give away valuable personal information. For example, a user name of Hannah1199 might indicate you have a daughter named Hannah born in November 1999. Do you really want strangers knowing that?
- **Beware of "phishing."** With this scam, companies use email or fake websites to collect personal information from consumers. Thousands of consumers have fallen victim to the "PayPal" and "BestBuy" email scams, for example, where they allegedly received emails from these companies, asking them to log in and update their information.

  The sites were operated by fraudsters, but looked real. Always log into financial sites from the home page you usually use, and check out suspicious emails at sites devoted to exposing email hoaxes, such as http://hoaxbusters.ciac.org/ or www.truthorfiction.org before responding to emails like this.
- **Think twice before providing sensitive personal information online.** In some scams, consumers have been duped into "applying for loans" on fake websites designed only to gather consumer information. In other cases, companies have sold information gathered from consumers, without their permission, to outside companies. Make sure the website is

reputable before you type in your social security number or other identifying information.

- **Free isn't always good.** Another recent scam involves sites offering "free" credit reports, which instead harvest information that can be used for identity theft. Visit the Federal Trade Commission's website at www.ftc.gov for more information on how to protect yourself from this scam.
- **Shop carefully.** Deal with merchants that have secure websites, and are reputable. For the maximum protection, always use a credit card rather than debit or check card when dealing with a new merchant online.
- **Teach your children** about online privacy and make sure they understand they are not to give out any personal information without your permission first.
- **Before you trash a computer,** make sure your information is no longer available to someone who may pick it up from the trash or a charity. Purchase a program that "wipes" your computer clean or physically destroy the hard drive. (Simply deleting files will not be sufficient.)

What to Do if It Happens to You

If you have been a victim of identity theft, you'll want to take these steps immediately:

- **File a police report.** You'll need this to report the theft. Keep the original and make copies for others who need it.
- **Notify the credit bureaus.** Report the fraud immediately to the three major credit reporting agencies – Equifax, Experian and TransUnion. One company should notify the other two but be sure to ask. Ask that a "fraud alert" be placed on your file. (See How the New Credit Reporting Law can help).
- **Fill out a fraud affidavit form.** You can get a standard fraud affidavit form at the Federal Trade Commission (FTC)'s website: www.ftc.gov/bcp/conline/pubs/credit/affidavit.pdf.
- **Order your credit report.** By law, fraud victims are currently entitled to one free copy of their credit report.
- **Contact your issuers.** If you suspect that your current accounts (especially credit cards) are being used, contact your creditors and ask that those accounts be cancelled. This also applies to your ATM card or check cards.
- **Investigate new accounts**. Review your credit report, preferably from all three major bureaus, and contact all unknown creditors listed under New Accounts or Inquiries. Explain that you are an ID Theft victim and ask them how you can file a report. They'll likely want a fraud affidavit, proof of your identity, and a copy of the police report.
- **Check your address.** Check with the Postal Inspector to see if a change of address has been filed. Also notify them if you suspect the imposter has used the U.S. mail in their crime (for example, if they have mailed change of address notices or credit applications).
- **Check your checks.** One unsuspecting consumer bought magazines from a young door-to-door salesman. Within hours, a fraud ring had made up fake checks and was going on a spending spree with his account. If you suspect that your checks are being used fraudulently contact the major credit verification bureaus to file a fraud alert:
- Chexsystems is the largest check company providing this type of service. Contact them at www.chexhelp.com and click on the "report identity theft" button or call 1-800-428-9623.
- Telecheck is smaller but it may also be helpful to contact them: www.telecheck.com or 1-800-366-2425.
- **Double-check your driver's license.** Contact your state's Department of Motor Vehicles to place a fraud alert on your driver's license, if you suspect it has been misused in any way. Recent investigative reports have shown it is very easy for imposters to get new driver's licenses using other people's information.
- **Contact the Social Security Administration** if you think your social security number has been used fraudulently. Even if you aren't sure, review your Benefits and Earnings statement to make sure it's accurate. Think twice about requesting a new social security number, however, since this can create more problems than it solves. You can report fraud to the SSA at (800) 269-0271 or visit www.ssa.gov.
- **Check your passport.** Alert the passport office to make sure no one orders a passport with your information (either a replacement or a new one). Visit http://travel.state.gov or call 1-877-4USA-PPT (1-877-487-2778).
- **Talk to an attorney.** Under the credit reporting law you have only two years after you discover misuse of your credit report to bring a lawsuit. You may want to talk with an attorney if you run into roadblocks with either credit reporting agencies or creditors. Contact the National Association of Consumer Advocates at www.naca.net to locate an attorney in your area

with experience in the Fair Credit Reporting Act and identity theft cases. What if you know the thief? Many times consumers know the thief that stole their information. It may be a coworker, friend or even a relative or loved one. This can create additional problems since the victim is afraid of getting the thief in trouble with the law. Identity theft is a serious crime, however, and if you do not handle the situation appropriately you may be stuck with the after-effects for years to come. For helpful guidelines describing what to do when you know the criminal, visit the ID Theft Resource Center at http://www.idtheftcenter.org.

How the Credit Reporting Law Can Help

In 2003, Congress passed a law updating the federal Fair Credit Reporting Act. It contains an entire section of requirements to make it easier for fraud victims to resolve their case. Here are some of the highlights.

Identity Theft Fraud Alerts

If you think you may have been, or are about to be, a victim of identity theft, credit reporting agencies must place a fraud alert on your credit report if you request it. There will be a system in place so that you should only have to make one phone call to initiate this. You will have to fill out a fraud affidavit and provide proof of your identity. Members of the military on active duty may request an alert placed on their file indicating they are on active duty. For those with fraud alerts on their credit files, creditors will have to take reasonable steps to make sure they verify a consumer's identity.

Identity Theft Prevention

Federal banking agencies, the National Credit Union Administration, and the Federal Trade Commission will work together to develop guidelines for creditors and others that use credit report information to prevent identity theft. They will also require financial institutions or users of credit reports to notify the Federal Trade Commission if there has been a security breach of consumer information.

They will also establish rules so that when a card issuer receives a request for a new or replacement card from a consumer less than 30 days after receiving a change of address, the issuer will have to take additional steps to verify that the request is valid. You'll also be able to ask the credit bureaus not to disclose the first five digits of your social security number when they supply your credit report.

If Your Identity Has Been Stolen

If you do become a victim of identity theft, you'll be able to request a copy of any application and transaction records related to any business transaction that was made by the imposter. For example, you can request copies of the application from a card company that opened an account for the thief in your name. You'll have to provide proof of your identity and, if the business requests it, a copy of a police report and an identity theft affidavit. The business will have to supply this information within 20 days. Within four business days of notifying a credit reporting agency of identity theft, the bureau must block the information that the consumer reports is fraudulent and notify the creditor reporting the information that the consumer believes it's fraudulent. (By the way, there are safeguards built in the law so that consumers can't use this provision to fraudulently boost their credit.)

Identity theft victims can get two free credit reports in the year, as well as have their file blocked from prescreened credit offers. Creditors will also be required to follow certain procedures to make sure that information that has been blocked or removed can't be resubmitted to the credit bureau again. The goal is to keep information legitimately related to identity theft off the consumer's report. Creditors also generally can't sell or transfer accounts that consumers claim are due to identity theft — most importantly to collection agencies. Debt collectors who are notified that a debt may be related to identity theft must notify the creditor from whom they received the debt that it may be fraudulent and provide information required by law. You'll have up to two years after you discover that you've been a victim of identity theft, but no longer than five years from when it occurred, to bring a lawsuit related to this law.

Additional Resources

Several websites provide additional helpful information for both preventing and dealing with identity theft:

Federal Trade Commission: www.consumer.gov/idtheft/
Identity Theft Resource Center: www.idtheftcenter.org
Privacy Rights Center: www.privacyrights.org

Notes

Notes

KFE

Knowledge of Financial Education

A product of CONSOLIDATED CREDIT

R-011518