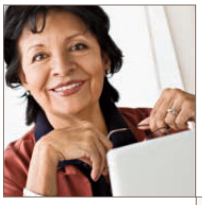
ID Theft Protection Kit

EQUIFAX®

Congratulations.

You've taken a big step in protecting the power of your credit … and your identity.

Identity theft is a serious crime. Victims can spend a significant amount of time and money to clean up the mess thieves have made of their good names and their credit. In some cases, victims have lost job opportunities or been turned down for mortgages or other loans. Now you have a useful tool to minimize the impact identity theft can have on your life. Keep reading for information on the steps you can take to protect your identity and what to do if you become a victim.



Contents

1.0 Identity Theft Basics

I. What Is Identity Theft?

Identity theft occurs when someone steals your personal information — to take over your credit accounts, to open new ones, to take out a loan, to rent an apartment, to access bank accounts, or to commit many other crimes using your identity. When identity theft strikes, the effects can be devastating. What's more, because it frequently involves no physical theft, identity theft may not be noticed by its victims until significant damage has been done, potentially several months and thousands of dollars later.

How Do Thieves Do It?

First, they steal your personal information by …

- Going through your mail or trash, looking for bank and credit card statements, pre-approved credit offers, and tax information.
- Stealing personal information from your wallet or purse, such as identification, and credit or bank cards.
- Completing change-of-address forms to redirect your mail.
- Acquiring personal information you share over unsecured sites on the Internet.
- Buying personal information about you from an inside source. For example, a store employee may get your information from a credit application or by "skimming" your credit card when you make a purchase.
- Accessing your personnel records at work.

Then, they use your personal information by …

- Opening new credit card accounts using your name, date of birth, and Social Security Number. When they use these credit cards and do not pay the bills, the delinquency is reported on your credit report.
- Establishing phone or cellular service in your name.
- Opening a bank account in your name and writing bad checks on the account.
- Counterfeiting checks or debit cards and draining your bank account.
- Buying cars by taking out auto loans in your name.
- Calling your credit card issuer and pretending to be you, changing the address on the account, requesting new cards be issued and the credit limit increased. Bills get sent to the new address, so you do not realize there is a problem until you check your credit report.
- Filing for bankruptcy using your name to avoid paying debts they have incurred under your name.

Identity Theft Statistics

The 2010 Identity Fraud Survey Report published by Javelin Strategy and Research reports that in 2009:

- 11,100,000 adults became ID fraud victims (4.8% of the U.S. population)
- The total annual fraud amount was $54 billion.

Sources: Javelin Strategy and Research, 2010, Identity Fraud Survey Report

II. Ten Important Steps You Can Take to Prevent Yourself from Becoming A Victim of Identity and to Minimize the Potential Damage

According to the 2010 Javelin Identity Fraud Survey Report, there is an upturn in fraudsters targeting consumers' existing credit card accounts, and opening new accounts with stolen information.

Unfortunately, it is not possible to prevent identity theft and credit fraud entirely, but by managing your personal information carefully, you can substantially reduce the likelihood that theft will happen to you. The following are some of the things you can do:

1. Lock your Equifax credit file

Equifax Credit Report Control™[1], found in Equifax Complete Premier™, and other selected products lets you decide whether your Equifax credit file can be accessed (certain exceptions apply*), and keeping your Equifax credit file locked can help prevent identity thieves from getting credit in your name. This feature gives you greater protection and peace of mind because companies will not be able to pull your credit report without your authorization. When you are applying for loans or credit, Equifax Credit Report Control allows you and only you to unlock your Equifax credit file for a period of time, or even for specific companies. You can also make changes to your lock status online or over the phone when you are on the go.

[1]Equifax is pleased to provide this information for your convenience, however it is provided for informational purposes only and does not constitute professional or legal advice of any kind or description. The information contained in these materials is believed to be reliable at the time it was written but it cannot be guaranteed in so far as it is applied to any particular individual or situation.

1.0 Identity Theft Basics

2. Place fraud alerts on your credit file

Equifax includes a free Automatic Fraud Alert* feature with Equifax Complete Premier and selected other products. This feature allows you to place an initial 90-day fraud alert on your Equifax credit file which will then be referred to the other nationwide credit reporting agencies. A fraud alert on your credit file is a good way to help prevent identity theft, as it notifies lenders that they should take steps to verify your identity, such as by contacting you before authorizing new or additional credit.

** The Automatic Fraud Alert feature is made available to consumers by Equifax Information Services LLC and is fulfilled on its behalf by Equifax Consumer Services LLC.*

3. Scan the Internet for your personal information with WebDetect™[2]

You probably already know your identity is one of your most valuable assets, but are you aware that thieves are buying complete identities — including names, Social Security Numbers, functioning credit card numbers and more — for as little as a few dollars? The trend in thieves getting information on suspected underground Internet trading sites continues to rise.** This escalation has allowed criminals to buy personal information in bulk, putting more and more people at risk of identity theft.

According to the FBI and the National White Collar Crime Center, Americans in 2009 reported losses of $559 million as a result of online fraud, with average losses running around $575.‡ As identity thieves become savvier, some have recruited hackers to defraud consumers of personal information. The stolen data is usually sold through instant-message groups or online forums that last only hours or days, to avoid being tracked by authorities.

Now you can take action to help protect yourself against this new kind of identity theft. Equifax Complete Premier includes WebDetect. This product scans suspected Internet trading sites and chat rooms for your Social Security Number (if elected) and up to 10 major credit and debit card numbers you provide, alerting you if your sensitive personal information is found on suspected trading sites. Just visit Equifax.com to learn more.

***Robertson, Jordan. "Online Crooks Face Tough Competition." Washington Post. 8 April 2008.*

‡ Internet Crime Complaint Center. "2009 Internet Crime Report."

4. Monitor your credit

Checking your credit report can help you identify potentially fraudulent activity before it wreaks havoc on your personal finances. Make sure your report is accurate and includes only those activities you can explain.

It is also a good idea to review your credit report from each of the three major credit reporting agencies every year, as it is possible that information is reported to one but not the others.

Think about monitoring your credit like having a smoke detector in your home. It is not something you turn on once in a while; you keep it on, knowing it will alert you when there are problems. Key changes to your credit file will help you quickly identify potential problems. This is especially important given the amount of and speed at which personal information is exchanged today. Enrolling in a credit monitoring product like Equifax Complete Advantage or Equifax Complete Premier takes the worry out of protecting your credit file, by notifying you within 24 hours of key changes that could be the early warning signs of identity theft.*

5. Be careful when giving out your personal information

Whether on the phone, by mail, or on the Internet, never give anyone your credit card number, Social Security Number, or other personal information for a purpose you do not understand. Ask to use other types of identifiers when possible, and do not carry your Social Security card. Be sure to keep it in a secure place.

6. Protect your documents and mail

To stop a thief from going through your trash or recycling bin to get your personal information, shred your charge receipts, credit applications, insurance forms, bank statements, expired charge cards, and pre-approved credit offers. You can help reduce your risk by choosing to opt-out of pre-approved offers of credit or insurance products by calling 1-888-567-8688. Deposit outgoing mail in post office collection boxes or at your local post office. Promptly remove mail from your mailbox after it is delivered. If you plan to be away from home, call the U.S. Postal Service at 1-800-275-8777 or go to www.usps.com and request a vacation hold on your mail delivery.

[2]Equifax is pleased to provide this information for your convenience, however it is provided for informational purposes only and does not constitute professional or legal advice of any kind or description. The information contained in these materials is believed to be reliable at the time it was written but it cannot be guaranteed in so far as it is applied to any particular individual or situation.

1.0 Identity Theft Basics

7. Guard your credit cards and PINs/passwords

Minimize the information and the number of cards you carry in your wallet. Do not keep personal identification numbers (PINs) or other credit card access codes with your credit card. If you lose a card, contact the fraud division of the credit card company immediately. If you apply for a new credit card and it does not arrive in a reasonable period, contact the issuer. Watch cashiers when you give them your card for a purchase. Also, when you receive a new card, sign it in permanent ink and activate it immediately. Memorize your passwords and PINs instead of carrying them with you. Avoid using easily available information passwords, like your mother's maiden name, your birth date, the last four digits of your Social Security Number or phone number, or a series of consecutive numbers.

8. Pay attention to billing cycles

Contact lenders immediately if your bills arrive late. A missing bill could mean an identity thief has taken over your credit card account and changed your billing address.

9. Safeguard personal information in your home

Make sure that sensitive personal information, such as bank statements, Social Security paperwork, passports, etc., is stored in a safe place in your home. If you have a service appointment requiring outside help to enter your residence, pay special attention to ensure your personal information is secure. If you are unable to be at home for the duration of the appointment, consider asking a friend or family member to help.

10. Protect your computer

Viruses and other malware are rampant on the Internet, so keep your anti-virus software up-to-date. Use caution when downloading information, and be sure you know that the source is credible. When downloading e-mail attachments, perform a virus scan first — even if you know the person who sent it to you -- as his or her own e-mail account may have been compromised.

III. What to Do If You Are a Victim of Identity Theft

If you suspect that someone has used your name, Social Security Number, or other personal information to get credit or a loan, the following information can help you:

Keep a record

Recovering from identity theft can be a long and complicated process, so it is important to keep a record of all communications. Send all letters by certified mail and keep copies. If you think your case might lead to a lawsuit, keep track of how much time you spend dealing with the problem.

Call the police

Report the crime to the police or sheriff's department that has jurisdiction in your case and request a police report. Though the authorities may be limited in what they can do to help, a report may be necessary to help convince lenders that someone else has opened an account in your name.

Check your credit report

Get your credit report from each of the three nationwide credit reporting agencies and check for any new accounts opened in your name. Because new accounts may take up to six months to show up on the report, continue to monitor your credit reports. A Three-Bureau Credit Report from Equifax will give you a line by line comparison of your credit history as reported to Equifax, Experian, and TransUnion.

Contact any of the credit reporting agencies

Contact any one of the three nationwide credit reporting agencies and request that an initial 90 day fraud alert be placed on your credit file. Once your alert is placed on your credit file at one of the nationwide credit reporting agencies, it will automatically be forwarded to the other two so that you do not need to contact each of them separately.

Subscribe to a credit monitoring product

Products like Equifax Complete Advantage or Equifax Complete Premier monitor activity in your credit file. When there are changes to key information, like when new credit accounts are applied for in your name, you receive an alert. You can then view the alert, which will describe the change to your credit file, so that you can make sure it is not the result of identity theft or fraud. You can also help prevent identity theft from taking place by using the Automatic Fraud Alert feature (included with Equifax Complete Premier), which enables you to place a fraud alert on your Equifax credit file (and referred to the other nationwide credit reporting agencies) and is automatically renewed every 90 days. This prompts lenders to take steps to verify your identity, such as by

contacting you before authorizing new or additional credit.

Visit www.equifax.com to learn more about Equifax identity and credit monitoring products.

IV. Victims' Rights

If you have been a victim of identity theft, you have certain rights. Here is a brief summary of the rights designed to help you recover from identity theft:

Fraud alerts

You have the right to ask that the major credit reporting agencies place a "fraud alert" in your file to let potential creditors and others know that you may be a victim of identity theft. There are two types of fraud alerts: an initial fraud alert that lasts for 90 days and an extended fraud alert that lasts for 7 years. You can place an initial fraud alert on your Equifax credit file 24 hours a day, 7 days a week online by going to www.alerts.equifax.com or by calling our auto fraud line at 1-888-766-0008 and following the prompts. Once placed with Equifax, the other two major credit reporting agencies, Experian and TransUnion, will be notified as well. You may place an extended 7-year alert by writing to Equifax or to one of the other nationwide credit reporting companies and providing an Identity Theft Report, as well as a day and evening telephone number. The requirements for an Identity Theft Report are listed on the FTC's web site at www.ftc.gov. The extended alert removes your name from pre-screened offers of credit for 5 years. If you currently subscribe to Equifax Complete Premier, you may use the free Automatic Fraud Alert feature within your product which places a fraud alert on your Equifax credit file (and referred to the other nationwide credit reporting agencies) and automatically renews every 90 days.

Equifax Fraud Alert
Phone Number: 1-888-766-0008
Or go online: www.alerts.equifax.com

Credit report

When you place a fraud alert on your credit file, you have the right to free copies of the information in your file (your "file disclosure"). An initial fraud alert entitles you to a copy of all the information in your file at each of the three nationwide agencies, and an extended alert entitles you to two free file disclosures in a 12-month period following the placing of the alert. You can obtain your free fraud alert credit file disclosure from Equifax at www.alerts.equifax.com

You also have a right to obtain a free copy of your credit report once every 12 months from each of the major nationwide consumer reporting companies. To order your free annual report from one or all the national consumer reporting companies, visit www.annualcreditreport.com, call toll-free 1-877-322-8228, or complete the Annual Credit Report Request Form and mail it to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

Fraudulent information

You have the right to obtain certain documentation relating to fraudulent transactions or to accounts opened using your personal information. A creditor or other business must give you copies of applications and other business records relating to transactions and accounts that resulted from the theft of your identity, if you ask for them in writing and include the information required to respond to your request. You will be required to provide proof of your identity and proof of your claim of identity theft (including both a police report and an affidavit) before a business can give you this information.

Reporting information to consumer reporting agencies

You also may prevent businesses from reporting information about you to consumer reporting agencies if you believe the information is a result of identity theft. To do so, you must send your request to the address specified by the business that reports the information to the consumer reporting agency. The business will expect you to identify what information you do not want reported, to provide an identity theft report, and to write a letter explaining that the information that they are reporting resulted from identity theft. Note that the information provider may continue to report the information if later it is learned that the information does not result from identity theft.

Blocking consumer reporting agencies from reporting information in your credit file

If you believe information in your file results from identity theft, you have the right to ask that a consumer reporting agency block that information from your file. An identity thief may run up bills in your name and not pay them. Information about the unpaid bills may appear on your credit report. Should you decide to ask a consumer reporting agency to block the reporting of this information, you must identify the information to block and provide

2.0 List of Resources

the consumer reporting agency with proof of your identity and a copy of your identity theft report. Once the consumer reporting agency has accepted your identity theft report, it must notify the information provider about the block. If a consumer reporting agency tells an information provider that it has blocked fraudulent information in your credit report, the information provider may not continue to report that information to the consumer reporting agency. The information provider also may not collect the debt that relates to the fraudulent account, or sell that debt to anyone else who would try to collect it.

Helpful Resources

There are a number of additional services available if you believe you have been a victim of identity theft:

Credit Reporting Bureaus

Equifax
P.O. Box 105069, Atlanta, GA 30348
Report fraud: Call 1-800-525-6285 or write to address above.
Order credit report: 1-800-685-1111
www.equifax.com

Experian (formerly TRW)
P.O. Box 9532, Allen, TX 75013
Report fraud: Call 1-888-397-3742 or write to address above.
Order credit report: 1-888-397-3742
www.experian.com

TransUnion
P.O. Box 6790, Fullerton, CA 92834
Report fraud: 1-800-680-7289 and write to address above.
Order credit report: 1-800-888-4213
www.transunion.com

Other Resources

Federal Trade Commission (FTC)
The FTC offers information for victims. File your case with the FTCConsumer Response Center. Include your police report number.
Use the FTC uniform affidavit form.
1-877-438-4338
www.ftc.gov/idtheft

Social Security Administration's Fraud Hotline
800-269-0271

If you want to know more about identity theft and credit fraud, the following nonprofit Web sites are excellent sources of information and additional contact information.

US Government Web site for Identity Theft
http://www.ftc.gov/idtheft

FTC Consumer Complaint Form
https://www.ftc.gov/ftc/cmplanding.shtm

US Department of Justice:
http://www.usdoj.gov/criminal/fraud/websites/idtheft.html

Social Security Administration/Office of the Inspector General Fraud Web site
http://www.ssa.gov/oig/guidelin.htm

US Secret Service: What to do if you're a victim of identity theft
http://www.secretservice.gov/criminal.shtml

ID thieves are always on the lookout for new ways to obtain your sensitive personal information. It is critical that you stay one step ahead, and one of the easiest and most effective ways is to remain educated and up-to-date regarding identity thieves' latest techniques.

By knowing what to look for, you can make better choices to protect your identity. Whether it is a scam involving social media sites, obtaining data while performing civic duties, or other types of malicious attack, identity thieves will try and take advantage of any way they can secure your sensitive personal information. Here's a selection of recent scams and techniques to know what you should be on the lookout for:

Gadget Grifters:

One of the growing types of identity theft involves stealing information through our electronic gadgets. As society becomes increasingly "wired," it is becoming easier to gain access to sensitive personal information on the go. Criminals can use mobile devices to their advantage in a number of ways. If you are not careful when using your credit card, a thief could easily and discreetly take a picture of your card with his/her camera phone. Similarly, it is important to watch out for peering eyes if using your computer in public. In general, take steps to safeguard your belongings; the more personal information we store on our electronic devices, the more vulnerable we leave ourselves to identity theft if those devices are misplaced or stolen. The best way to safeguard against these kinds of crimes is to be discreet when paying with a credit card to prevent any unwanted eyes from seeing it. Additionally, make sure you use secure sites on your wireless devices and clear all personal data from them when you are finished with your transactions. You could also consider utilizing password protection on your phone and laptop.

3.0 Latest Trends in Identity Theft

Tech Tactics

Identity thieves are always developing new ways to obtain sensitive personal information over the Internet. While you may have heard of phishing (fraudulent e-mails disguised as if they were from trusted sources to obtain personal information) and pharming (redirecting Web traffic to fraudulent sites to obtain information), you should also be conscious of IP spoofing.

IP spoofing, or Internet Protocol spoofing, is a technique used to gain unauthorized access to computers by tricking the computer itself into thinking the hacker's IP is a "safe" one. Once this is accomplished, the hacker could have full access to your computer — without you even knowing. The best way to avoid this sort of fraud is by making sure your computer's security programs are up-to-date and by utilizing the most secure filter, router, or firewall offered.

New Twists on Old Techniques

Identity thieves have relied on credit card scams for quite a while, but current economic challenges have allowed them to use new, more successful angles to get the information they need. Due to tightened credit, criminals are advertising fraudulent credit offers to victims who may be strapped for cash but are not qualified to apply for credit (poor credit score, lacking a SSN).

They can also obtain sensitive personal information by posing as debt consolidation experts or by offering to obtain lower interest rates for the victims. Make sure that all credit interactions you have are with reputable sources.

You can always turn to the Better Business Bureau if you are unsure.

Staying Safe Socially

With the rapidly growing popularity of social media sites, more people are sharing an increasing amount of personal information over the Internet. Even if you do not consider some of the information you display on social sites "sensitive personal information," you should still use strict privacy settings.

Numerous studies have shown that with the right technology, determined identity thieves may be able to eventually piece together seemingly insignificant facts about you along with publicly available information to steal your identity. The best way to prevent this is to share as little information publically as possible and ask that your friends be subtle in the information they share about you; your best efforts to safeguard your identity can be negated by a careless friend's wall posts.

The Jury Duty Scam

Identity thieves often prey on people's fear and , in some cases, their civic obligations. The "Jury Duty" scam, for example, is remarkably easy to fall for. Imagine this scenario: you receive a call from a jury coordinator informing you that a warrant has been issued for your arrest due to your failure to appear for jury duty. When you explain that you never even received a summons for jury duty, the coordinator asks for your Social Security Number and date of birth in order to verify your information and cancel the warrant. Of course you are willing to provide this information; there has obviously been a mistake and you want to avoid arrest at all costs. The problem is, this is all part of the scam. There never was a warrant, and you have just had your identity stolen.

This scam has been reported in a number of states. So if you receive a phone call that seems suspicious or threatening, do not panic. Simply ask for more information, the caller's supervisor, or a number at which you can reach them after doing more research. Nothing foils an identity thief like an educated response.

[1]Equifax Credit Report Control is only available while you have a current subscription to an ID Patrol, Equifax Complete Advantage or Equifax Complete Premier product. Locking your credit file with Equifax Credit Report Control will prevent access to your Equifax credit file by certain third parties, such as credit grantors or other companies and agencies. Credit Report Control will not prevent access to your credit file at any other credit reporting agency, and will not prevent access to your Equifax credit file by companies like Equifax Personal Solutions which provide you with access to your credit report or credit score or monitor your credit file; Federal, state and local government agencies; companies reviewing your application for employment; companies that have a current account or relationship with you, and collection agencies acting on behalf of those whom you owe; for fraud detection and prevention purposes; and companies that wish to make pre-approved offers of credit or insurance to you. To opt out of such pre-approved offers, call 1-888-567-868

[2]WebDetect can scan suspected internet trading sites for your Social Security number (if you choose to) or up to 10 major credit/debit card numbers you provide. Because the addresses of the suspected internet trading sites searched by WebDetect are not published and frequently change, there is no guarantee that WebDetect is able to locate every possible internet site where consumers' personal information is at risk of being traded. Your Social Security number or the credit card numbers you have chosen to scan for with WebDetect may be at risk of being traded on the internet even if you do not receive a WebDetect alert.

Equifax Dedicated Customer Support

1-800-4EQUIFAX

24 Hours a Day

7 Days a Week