Identity Theft
February 2013

Introduction

The purpose of this document is to provide some basic information about Identity Theft including its definition and a list of things you can do to help prevent it. Also provided below are a number of Web sites where you can obtain additional information. A list of several Identity Theft Protection Services is provided should you want to spend the money for the increased protection that they claim to provide.

If you choose not to subscribe to one of these services there are steps that you can take on your own that will go a long way towards protecting your identity. In summary, this document will provide you with sufficient information to make educated choices provided you read through it and do sufficient research on your own or consult with qualified experts.

Note: To take full advantage of this document you should allow yourself an hour or so a day for several days to visit all of the referenced Web sites and to do your own research. Only then, will you be able to make informed decisions.

If you want to skip to the Short Course at the end of this document be sure to come back and read the details.

What got me started on this topic

- I read an article in Wired magazine which is available here. You should read it thoroughly.
- Also, I stumbled onto the information at https://www.privacyrights.org/ , it's a great site.

What is Identity Theft

Identity theft generally takes two forms: "account takeover," which occurs when the thief uses the victim's existing financial accounts to buy things; and "application fraud," which is when the thief uses the victim's personal information to create new accounts — or even a whole new life — in the identity theft victim's name. ***Identity Theft Protection services generally only protect against the latter.***

What is vulnerable?

Anything residing in, entering or leaving your house or your person such as:

1. Computer traffic including Email either incoming or outgoing
2. Wireless devices including Bluetooth and Wi-Fi
3. Mailbox, either incoming or outgoing
4. Phone – be careful what you reveal
5. Wallet contents
6. Paper lying around the house or in an unsecured file drawer

Identity theft scenarios

Check out the following for an idea of how identity theft can happen, as well as what can happen to your financial standing:

- John Doe sets up a phony website that claims to offer "discounts on prescription drugs." Jerry Smith responds to a phishing e-mail from the website, visits the site to place an order, and enters the requested information, including his credit card number. Mr. Doe collects the data from the website and goes on a shopping spree with Mr. Smith's credit card. The credit card issuer then attempts to collect payment from Mr. Smith for Mr. Doe's purchases.
- Jane Doe steals her sister Mary's credit card number. Jane uses Mary's card number to buy a plane ticket across country, put a security deposit on a new apartment, and buy items for her new home. All of these purchases will appear as charges on Mary's credit card statement.
- Jack Loe moves from one home to another but fails to notify the post office, his bank and others of his change of address. Tom Green moves into Jack's old home, then opens Mr. Loe's mailed bank statements and uses that information to transfer money from Mr. Loe's bank account to a new account in Mr. Loe's name that Mr. Green created.
- You receive a call from "MasterCard". It works like this: Person calling says, "This is Carl Patterson (any name) and I'm calling from the Security and Fraud department at VISA. My Badge number is 12460. Your card has been flagged for an unusual purchase pattern, and I'm calling to verify. This would be on your VISA card. Did you purchase an Anti-Telemarketing Device for $497.99 from a marketing company based in Arizona?"

  When you say "No". The caller continues with, "Then we will be issuing a credit to your account. This is a company we have been watching and the charges range from $297 to $497, just under the $500 purchase pattern that flags most cards. Before your next statement, the credit will be sent to (gives you your address), is that correct?"

  Caller then says he "needs to verify you are in possession of your card. Turn the card over. There are 7 numbers; first 4 are 1234 (whatever) the next 3 are the security numbers that verify you are in possession of the card. These are the numbers you use to make internet purchases to prove you have the card. Read me the 3 numbers." Then he says "That is correct. I just needed to verify that the card has not been lost or stolen, and that you still have your card. Do you have any other questions? Don't hesitate to call back if you do." ***Once you tell the caller the 3 numbers you are toast***.

These are just a few of the ways that identity theft can occur. Basically, any document you have, any unsecure website you visit, any conversation you have on a cordless or cell phone that contains personal, identifying information about you can be used by a thief to take possession of your identity.

Stopping Identity Theft

All is not lost, though: You can still uncover identity theft if you're willing to monitor your financial records regularly. Your credit reports can show unauthorized activity made in your name; so can your bank and credit card statements, depending on how the identity thief targets you. There are also programs available that can alert you to changes in your credit report, and some credit card issuers

make an attempt to contact their customers if they detect unusual buying patterns or other signs of abnormal card usage.

Your first and best defense against identity theft, however, is personal vigilance — safeguarding your credit and debit cards, installing a firewall on your computer, protecting or shredding documents that contain your personal information, monitoring your credit report and other financial records, and turning down telephone or Internet offers that promise you the world in exchange for "just a little information about you." You can also find identity theft insurance that will cover you for certain costs associated with identity theft. Such insurance does nothing to stop identity theft from occurring in the first place, but it will help you stay pro-active about reporting identity theft.

Bottom line, you do not need to store your money in a mattress or commit your personal information to memory and/or destroy a seemingly vulnerable paper trail. Protecting yourself from the threat of identity theft generally involves some minor adjustments to your habits. With common sense and the proper protective steps, you can significantly reduce your personal risk of identity theft.

Read more here and here.

What to do if you think you're a victim

- Place a Fraud Alert with one of the 3 credit bureaus. They will notify the other 2. You can do this at https://www.experian.com/fraud/center.html. It's easiest to do this online.
- Contact your credit card companies, your bank and all other financial institutions.
- File a report with the FTC at https://www.ftccomplaintassistant.gov/. You can also call them at 1-877-438-4338
- Order a copy of your credit report from one of the major credit bureaus. You can start at https://www.annualcreditreport.com/cra/index.jsp. Review the report for signs of fraudulent activity.
- The combination of the FTC Report and the Police Report is an Identity Theft Report. Save the reference number after filing the FTC report.
- Bring a copy of the FTC Report to the police and file a report with them.
- Keep a written log of all phone conversations, discussions, etc.
- Follow all of the steps listed at https://www.privacyrights.org/fs/fs17a.htm.
- Read the document titled Taking Charge at http://www.consumer.ftc.gov/articles/pdf-0009-taking-charge.pdf.
- Visit Identity the Theft Resource Center (ITRC) at http://www.idtheftcenter.org/.

Major causes

- Lost, misplaced or stolen wallets or cell phones
- Stolen or compromised driver's license
- Burglaries - obvious
- Phishing - this is a popular scamming technique and the cause of many identity thefts. It involves sending unsolicited emails in an attempt to obtain your personal information.
- Read more: Identity Theft Causes | http://www.ehow.com/how-does_5519679_identity-theft-causes.html#ixzz2JTsCABVz

- Address change -This method of identity theft is relatively simple and hard to avoid. An identity thief may fill out a change of address at the post office, diverting your mail to some other location where they can easily retrieve it.
- Skimming - involves the use of a storage device to copy your credit or debit card information. Any clerk or salesperson could easily run your card through a skimming device before or after running it for your purchase without you noticing. Pay close attention to what is being done with your card; never let a clerk walk out of sight with your debit or credit card. It is also possible for thieves to place skimming devices over ATM slots so that they scan your card on its way into the ATM machine. These devices protrude from the machine and often look out of place with the ATM design
- Trash can or Dumpster diving - Another common cause of identity theft occurs when you fail to properly dispose of documents that contain your personal information, like bank statements or bills. Thieves will sift through trash cans and dumpsters to get this information. You should always shred important documents.
- Income Tax Returns – thieves use your Social Security to file false returns early in the tax season to get quick cash. This is easier than robbing a bank.

Protecting your identity

There are several approaches to protecting your identity:

1. Keep doing what you're doing plus follow the appropriate recommendations in this document.
2. Subscribe to an Identity Theft Protection service.
3. Create your own plan including placing Fraud Alerts and Credit Freezes with the 3 major credit bureaus.
4. A combination of any or all of the above.

The cost of the above can vary from an initial one-time charge of $5 per person for placing Credit Freezes to an annual cost of over $300 per person.

Glossary

- Fraud Alert - any creditor that is asked to extend credit is asked to contact the consumer by phone and verify that the credit application was not made by an identity thief. ***The merchant may or may not do this***.
- Credit Freeze or frequently referred to as a Credit Lock or Security Freeze. A security freeze prevents anyone from accessing your credit making it virtually impossible for anyone to open a line of credit, new credit card, etc. in your name. Even you have no access unless you remove the freeze. – see http://www.privacy.ca.gov/consumers/cis10english.pdf to place or remove a freeze on your Credit Files. Also read about it here. If you plan to purchase a car, open a new charge account, etc., you will have to unfreeze you credit. If you are tempted to open a charge account at Macys to save 10% on your next purchase, don't freeze your accounts. You need to consider the tradeoffs. Credit Freezes are best suited to seniors who don't require frequent access to credit bureaus.
- Key logger – a software program that enters your PC by way of a Trojan infection. This software monitors your keyboard activity and sends the data to thieves allowing them to learn your passwords,

etc. You can obtain anti-keylogger software from https://www.privacyprotect.com/ for $19.95 per year. You shouldn't need it if you scan periodically with antispyware software and keep your antivirus software up to date.

- Credit Bureau - an agency that collects, maintains, and sells individual credit information in the form of a credit report.
- Identity Theft Service - Identity theft protection services can help you monitor your accounts. They can place fraud alerts or freezes on your credit reports or remove your name from marketing mailing lists. Many people find it valuable and convenient to pay a company to keep track of their financial accounts, credit reports, and personal information. Other people choose to do this on their own for free. Before you pay for a service, evaluate it and its track record before you pay any fees.
- Credit Monitoring - Credit monitoring is, simply put, the act of closely watching your credit report for changes, such as inquiries made (a company accessing your credit report – lender, creditor, insurer etc.), or checking for signs that you have opened a new account… These are just some of the things that you should watch for, there are more which the some Credit Monitoring Service can help you with.
- Credit Score – see https://www.privacyrights.org/fs/fs6c-CreditScores.htm
- Internet Monitoring – some services scan all of the known black market sites for your credit card and other information
- Credit Report Alerts – protection services notify you when there is a change to your credit as a result of anyone trying to access your credit bureau information
- Fraudulent Withdrawal – someone uses your identity to make a bank withdrawal
- Secure Web sites - look for the https and lock symbol
- ITAC – Identity Theft Assistance Center at http://www.identitytheftassistance.org/
- Free Annual Credit Report – only go to www.annualcreditreport.com where you are entitled to one free credit report annually from each of the 3 Credit Bureaus and it's **free**.

Common Sense Tips

Although most of these tips are common sense and are widely known, this document would not be complete if they were omitted.

- Never give out any personal information or information on any credit card unless you initiated the call. If your credit card company calls and ask if you have your card in your possession, tell them you'll call them back using the number on the back of your card. The caller may be phishing for the 3-digit code on the back of your card.
- Make sure that all of your credit cards contain your photo and signature on the front of the card
- Place the contents of your wallet on a photocopy machine, do both sides of each license, credit card, etc. You will know what you had in your wallet and all of the account numbers and phone numbers to call and cancel. Keep the photocopy in a safe place. Make sure to use your own copier.
- Remember – anyone standing near you can take a photo of your credit card, driver's license or any other personal document. Just be on the alert.
- Credit Reports – you are entitled to three free credit reports annually. I recommend that you stagger them and choose a different bureau every four months. Use a reminder to prompt you. Keep your reports locked up. Go to https://www.annualcreditreport.com/cra/index.jsp and request your report. This is free for one report from each service annually.
- Avoid sites such as www.freecreditscore.com. Use www.annualcreditreport.comi Instead.

- Try not to favor convenience over security. One example is to use strong passwords rather than those that are easily remembered.
- User names – don't use your SS number for any user name or password.
- Checks – put the minimum required information on your checks. No SS number or Driver's license.
- Monitor credit card charges frequently, not just your monthly statement but learn how to access your credit card and banking accounts online.
- Find out what services and coverage your credit card company and bank provide relating to fraud.
- Do not leave your wallet, purse or cell phone in an unattended auto. If you go to the gym use the lockers provided by them and keep a casual eye out which is not always possible.
- Virtual Credit Card – use one when unsure about a particular online merchant.
- What information do you have to provide with a Credit Card or Check – see https://www.privacyrights.org/fs/fs15-mt.htm. It turns out that the answer is **not much**.
- Income Tax returns contain your entire identity – keep them secured. One way is to scan them and place them on a CD/DVD or Flashdrive for placing in a safe.
- Opt out of receiving offers of credit in the mail. You can click here to do this online or call 1-888-567-8688.
- Use a unique credit card for automatic payments – it's less likely to be compromised which saves a lot of hassle notifying merchants.
- Your passwords should be strong and not repeatedly used. They should not contain any words found in a dictionary. Use a Password Manager so that you only have to remember one password referred to as the Master Password.
- If you make any automatic payments from your credit card or checking account, keep a list in a safe place.
- Mailbox – remember, anyone can pilfer your mail both incoming and outgoing. Try not to have any correspondence either way by mail that contains any personal information.
- Trashcans should only contain shredded material.
- Don't publish anything online that reveals your identity such as on Facebook.
- Avoid Debit Cards; they are less secure than Credit Cards.
- Keep Social Security cards locked up and don't carry your SS number in your purse or wallet.
- If you lose your phone, remove the number from all banking profiles
- Driver's License – don't keep copies lying around.
- If you have a camera with a GPS and you post pictures on line, viewers may be able to find out where you live
- Online Banking – much safer than paper. Ask any security expert or your financial institution. Eliminate any statements from being mailed to you.
- Use a unique email address for your Gmail Recovery address
- Destroy all credit card receipts even though they only have the last 4 digits
- Some banks provide Identity Theft insurance as does Wells Fargo. It may be the law.

Computer Security

- Don't store any passwords, personal or financial data on you PC, ever. Always destroy all hard drives before recycling old PCs. Even printers and copiers can store some of your personal information. Most people don't realize this.
- For maximum security use the latest version of your Browser. If you still use Windows XP switch to Firefox or Google Chrome since you can't use the latest version of Internet Explorer.
- Be sure to back up all of you important files in case your PC becomes infected.

- Never go online without a Firewall and an up to date anti-virus. Read more at http://download.zonealarm.com/bin/media/pdf/defendTheNet_howToGuide.pdf.
- Make sure that your Operating System (Windows) and your anti-virus is kept up to date.
- Watch out for Key loggers – best defense is to scan with several antispyware programs periodically. TrustedID provides anti-keylogger software.
- Routers – be sure to use the built in security features. See the article at http://www.pcmag.com/article2/0,2817,1276349,00.asp.
- Secure browsing on the Internet - Many Web sites -- banks included -- use a transfer protocol called Hypertext Transfer Protocol Secure, or HTTPS. While we use HTTP on a daily basis to browse the World Wide Web, HTTPS adds a form of security that encrypts data. This security is typically depicted in your Web browser by a lock or key, and any secured URL should begin with "https://" instead of "http://". Next time you log into your online banking account, pay attention to your URL bar. Is the page encrypted? If so, it will be very difficult for anyone to eavesdrop on the connection and hijack your financial data.
- Unsecured Wi-Fi hotspots – avoid these for performing any online transactions unless you have a software firewall installed such as the free ZoneAlarm.
- For absolute safety, dedicate a single PC for online transactions. This is very inconvenient but you can get a $300 Notebook PC for this. Only use it for online banking, etc. This results in a spyware free PC.
- Always log off any site you visit even at home.
- Email – avoid attachments; don't ever provide any information to anyone via email. Don't fall for any phishing emails. Search Google for "phishing" to learn more.
- Flash drives – don't store any personal information of these unless it's encrypted. Even then I would avoid it.
- Practice save Surfing - Internet security is a multi-layered defense using several anti-spyware products (including an effective firewall) to supplement your anti-virus combined with common sense and safe surfing habits provides.
- Use a utility such as Darik's Boot and Nuke or CCleaner to erase a hard drive prior to disposing of it. It's available at http://www.dban.org/ or http://www.piriform.com/ccleaner. See the information here.
- Don't simply delete a file with personal data on it since it can be easily recovered. Instead, replace the contents of the file with zeros or gibberish and then delete it.
- Don't ever click a link in an e-mail to respond to any sort of inquiry. Either visit the Web site directly or call the call a company directly.
- Before using any Anti-Spyware product look it up at http://www.spywarewarrior.com/.
- Fraudulent charges made to your credit card while shopping online are limited to $50 by the Fair Credit Billing Act.
- When you use a payment service such as PayPal or Google Checkout you do not have to reveal your credit card number to online merchants.
- You can turn on Two-step verification with your Gmail account. You can go here or here to learn more.
- If you use LastPass they now have an Authenticator you can use. You can read more here.

Mobile Device Security

- Set up iCloud on your iPhone or iPad to enable Find My iPhone or iPad, and then sign in at icloud.com/find to locate your iPhone or iPad. See instructions at http://support.apple.com/kb/PH2698?viewlocale=en_US. You can also use the Carbonite Mobile App to locate your Andriod or Apple device.

- Andriod users can use the Carbonite Mobile App to not only locate your phone, but to wipe it remotely.
- Secure your phone with a Swipe Key code to prevent unauthorized access.
- Never leave your mobile device unattended even in a parked car.
- Record the IMEI number of your phone and serial numbers of all tablet devices in a safe place.
- Your Bluetooth wireless device is paired with your phone with a code as simple as 0000. This allows eavesdroppers to pair with your device by using this code. It's rare but it can happen. See a video about this at http://www.youtube.com/watch?v=1c-jzYAH2gw.

Identity Theft Protection Services

Who they are – you can find them through Google

- IdentityGuard
- AllClearID
- LifeLock
- TrustedID
- IdentityForce
- PrivacyGuard
- Wells Fargo 877-224-5790/7430 https://identity.wellsfargoprotection.com/
- And many others including your bank and credit card companies

How do they measure up

The two I liked the best were TrustedIT and IdentityGuard. I found LIfeLock a little pushy and expensive. Before selecting a service call them and see how long you wait on hold.

General Information

- The monthly charges run from $12.50 to $25 per month per person
- They are all somewhat misleading regarding the services they provide. You have to call several times since you get smarter after each phone call. They can tell that you have called more than once since they log your phone number even if you have caller IID blocking. Don't worry – just call until you have all of the info you need.
- You have to search extensively for the lowest rate for each service – see example above for IdentityGuard.
- Many of the services claim that if you use their service you don't need a Credit Freeze. I don't agree with this based on my research.

Is Identity Theft Protection necessary?

It depends on who you ask. Obviously, if you ask any of the major protection services they will say yes. In some cases it is difficult to get them to stop talking. It's your life so feel free to simply hang up.

Other opinions worth reading are here, here and here. You should definitely read these over before signing up for any service. You should definitely read the article here. For another viewpoint read the information here.

Remember, there's a difference between feeling good and feeling safe. I signed up for a trial subscription to a protection service and immediately felt good about it. I was amazed at all of the data that was immediately

placed at my disposal. But after a few days I asked myself if I was really safe enough. That is when I placed Fraud Alerts and Credit Freezes with the three Credit Bureaus on my own. The time required doing this for me and my wife was less than 30 minutes. I feel a little safer having done this.

Remember, there's a difference between fraudulent charges to an existing account and Identity Theft. Theft Protection Services do not prevent the former.

Online Reviews

- http://www.gotcredit.com/credit-monitoring-services
- http://www.nextadvisor.com/credit_report_monitoring/compare.php also
- http://identity-theft-protection-services-review.toptenreviews.com/
- http://www.identitytheftlabs.com/ - this is the best site for a listing of all possible services.

What they provide

Note – not all services provide all of these options. This is just a list to help you to ask more questions.

- Credit monitoring – they notify you of any changes to your credit within 24 hours. Note that this could be well after a thief opens a new account in your name.
- Fraudulent withdrawal insurance (rare)
- Credit scores (either 1 or 3 bureaus included)
- Credit Reports (updated at various periods based on service)
- Scanning of black market websites
- Fraud Alerts - most do not provide this but TrustedID provides a link for you to do it yourself
- Credit Freeze (TrustedID will do it for $29 per person. You can do it yourself for a total of $5). Many services do not provide this.
- Anti Keylogger software (IdentityGuard does provide this)
- Identtity Threat score (sort of generic and not extremely helpful)
- Anti-phishing and anti-spyware software
- Monitoring of public records
- Up to 30 day free trials
- Some sort of Insurance or Service Guarantee – be sure to ask for Terms and Conditions. It's not as good as it seems.

What they don't provide

- They do not protect any existing credit card, bank or brokerage accounts whatsoever
- Most of what's provided is after the fact. In other words, fraudulent credit card applications will be detected after the credit bureau is notified which can be anywhere from 24 hours on up.
- Each particular service omits one or more features so you will have to do extensive research.
- Most services do not place a freeze on your credit nor do they place fraud alerts

How things work

A person walks into BestBuy and sets up an account in your name. The store clerk is supposed to check with one of the Credit Bureaus. If you had previously placed a Fraud Alert with the 3 Credit Bureaus, BestBuy will receive a message that the clerk ***should*** call you to verify that it's really you. It's not mandatory. If they don't

contact you the perpetrator can open the new account. If you have your credit monitored, when BestBuy eventually checks your credit rating, your Identity Theft Protection Service will see this and notify you within 24 hours. By this time the perpetrator has made their purchase. On the other hand, if you had placed a Credit Freeze, the clerk will be unable to check the perpetrator's credit and should refuse the account.

Just FYI, brokerage accounts are not monitored by Credit Bureaus. Also, most banks guarantee your accounts against fraudulent withdrawals. Check with your bank.

If you place Credit Freezes with the 3 Credit Bureaus this doesn't provide any protection for existing credit cards, bank accounts or brokerage accounts. You should check with each of them to find out how you are protected against fraud. In most cases you are protected except for brokerage accounts which I have not gathered information about. Wells Fargo, as an example, provides protection against fraud as does CitiBank credit cards.

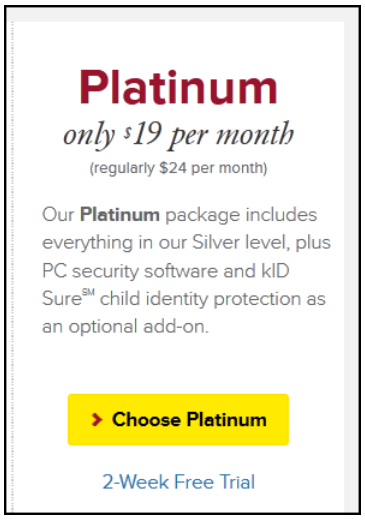
Signing up for any Identity Theft Protection Service does not prevent you from getting free reports from the credit bureaus.

If you add Identity Theft coverage to you Homeowner's policy, it usually covers losses or legal fees related to the fraud. It usually offers no preventive measures.

Pricing Example – it can be tricky

This example shows how you have to shop around before purchasing a plan. It's not pretty.

- Example – IdentityGuard
    - Web site at http://www.identityguard.com/compare-plans/ has the plan as shown below. This plan can be purchased for less if paid annually.



- Web site here has the plan as shown below

- Web site here has no price displayed but if you continue you'll see a $14.99 monthly cost
- If you call 888-548-7878 you can get a plan for $149.90 annually or $12.50 per month. This plan reduces the monthly credit report updates to quarterly instead of monthly.

Note: All of these services offer different plans which depend on how you get to their site. For example, you can get to IdentityGuard through Costco to buy the plan at $13.99 monthly with no annual payment discount option. The Web site is costco.identityguard.com.

List of Major Credit Bureaus

See all of their phone numbers at http://www.aprfinder.com/credit-bureau-phone-numbers .

- Equifax http://www.equifax.com/home/en_us
- Transunion http://www.transunion.com/
- Experian https://www.experian.com/

How to place a credit freeze

Most protection services do not place a freeze on your credit; you have to do it yourself. One exception is TrustedID who offer the service for $29 per person.
Read the information here first http://www.consumersunion.org/pdf/SecurityFreeze-Consider.pdf
The sites below allow you to place a freeze on your Credit Information and to remove the freeze either temporarily or permanently. There may or may not be a small charge. Unlike Fraud Alerts discussed below, Credit Freezes must be place at all 3 major Credit Bureaus for each person.
Go to the Web sites below.

Note – all Bureaus are slightly different and may ask to know previous addresses, etc. They all ask you for your SS number. It took me about 15 minutes to place a freeze on all 3 bureaus.

- EquiFax https://www.freeze.equifax.com/Freeze/jsp/SFF_PersonalIDInfo.jsp
  Cost is $5 per person
- Experian https://www.experian.com/freeze/center.html
  Cost is free
- TransUnion http://www.transunion.com/personal-credit/credit-disputes/credit-freezes.page
  Cost is free. Must set up an account.

How to place a Fraud Alert

Read the information here first. Note that Fraud Alerts must be renewed ***every 90 days*** and they are free.
Note – notifying one bureau will take care of all three of them.

- EquiFax http://www.equifax.com/answers/set-fraud-alerts/en_cp
- Experian https://www.experian.com/fraud/center.html
- TransUnion http://www.transunion.com/personal-credit/credit-disputes/fraud-alerts.page

Short Course

- Sign up for as many electronic transactions as you can. Avoid paperwork if possible.
- Never reveal any personal information over the phone unless you initiated the phone call.
- Don't carry more than one credit card in your wallet and keep your Social Security card locked up. This applies to Income Tax Returns as well. Use a credit card with your picture and signature on it.
- Don't click any links in an email; go to the web site on your own.
- Keep your PC up to date including Windows and your anti-virus. Scan periodically with a free antimalware program and make sure your Firewall is on.
- Sign up for Fraud Alerts and Freeze your Credit.
- Be vigilant. Review a free Credit Report every 4 months.
- Review your credit card accounts online at least weekly. Do the same for any checking or savings accounts.
- Scan both sides of everything that's in your wallet and keep it in a safe place.
- Keep passports locked away.
- Ask yourself how many times a week that your personal information comes in the mail or goes out. Aim for zero.
- Opt out of receiving offers of credit.
- And finally, if you want more piece of mind and possibly more protection sign up for an Identity Theft Protection Service.

Conclusions

If you don't need to see your Credit Scores and Credit Reports more than once every four months and feel like you have taken all of the precautions mentioned above and at Web sites referenced herein, you may not need to do anything. For a little extra protection you can place Fraud Alerts and Credit Freezes at the three major credit bureaus.

For additional peace of mind and approximately $150 annually per person you might want to consider a protection service. If you do not need frequent access to your credit and don't plan on taking out any new credit lines, don't let any protection service talk you out of freezing your credit. Read the Pro and Cons first at http://www.consumersunion.org/pdf/SecurityFreeze-Consider.pdf.