



# A Guide for Victims



## We're in this together

Identity Theft can be frightening, bewildering and confusing. Don't panic! We're here to help you from start to finish.

We understand the worry and frustration you may be feeling. We know what you need. We are committed to helping resolve your situation.

Your fraud specialist is committed to working closely with you until we achieve complete resolution to the best of our abilities, by coordinating communications with creditors, law enforcement, government agencies, gathering necessary documentation and preparing pertinent notification.

Be assured we are here to guide and assist you in every way possible. That is why you will be partnered with the same fraud specialist throughout the duration of your case.

We have many interesting articles, links to other information and tips on our website. Take a look!

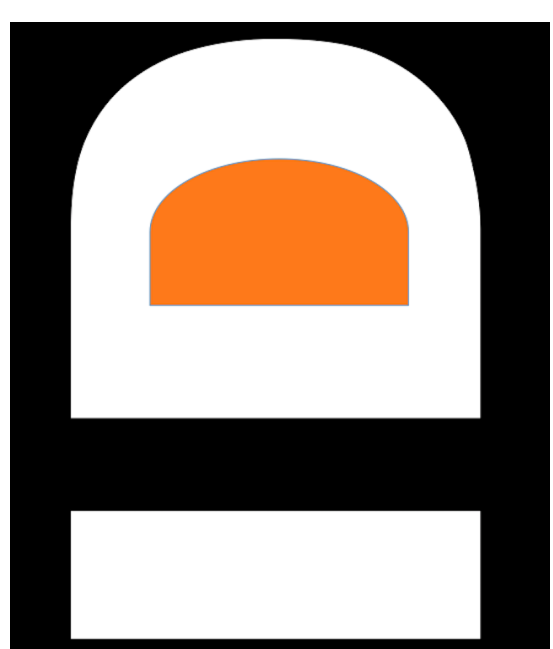
That's what we do and that's what we do best.



**Call us at 877 308 9169**  
**Visit us online [www.idresolution.net](http://www.idresolution.net)**

# Contents

- An Evolving Problem
- Your Systematic process for Identity Recovery
- The Larger Picture - Building a Case File
- Directions You should Follow
- How Did I Become A Victim?
- What If I lost Identity Documents?
- How Can I Protect Myself and My Family?





# Identity Theft is Constantly Evolving

Identity Theft is constantly morphing.

Whether it's different styles of attack (e.g. phishing or robocalling) or different patterns regarding target information (e.g. medical records or unemployment benefits, "card not present", etc), identity thieves and identity fraudsters are incredibly agile.

They want to go after the low hanging fruit and where possible do it in a scaled way.

Therefore we need to be constantly vigilant and do OUR part in protecting our valuable information.

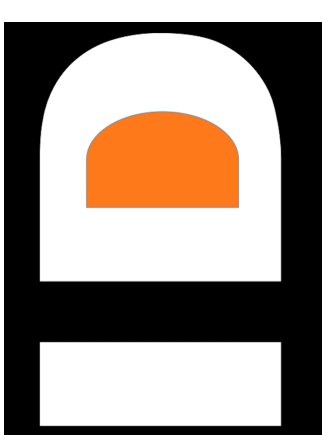
PIN Codes and Passwords, Social Media Access routes, Multiple Site Sign On's are all things we can protect by changing the way we access them and regularly upgrading passwords and PIN codes.

Dual Factor Authentication should be used wherever offered and NEVER use one password for multiple applications.

Keep abreast of current developments and go to our website to see useful articles, tips, and links to other useful information and websites.

Above all, remember this problem is not going to disappear in our digital age with more and more of our data online and interconnected.

Treat your personal information assets with the same care as you would your financial assets and you're off to a good start in staying safer.







# Your Process for Identity recovery

- **Law Enforcement Report**
- **ID Theft Affidavit**
- **Staying organized**
- **Identity and PII Monitoring**

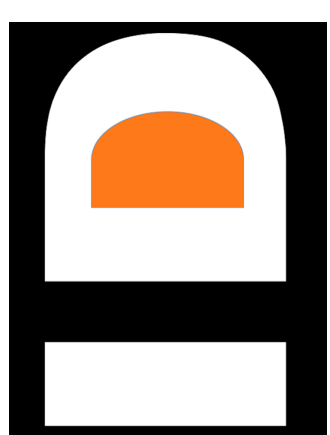
To begin the fraud resolution process, there are initial steps that need to be taken. Your fraud specialist will cover the listed steps below and assist you in this process. You may find that some of these steps have already been completed, which moves you one step further toward recovery.

The first step we need you to take is to file a law enforcement report – this is essential. We can help you, but the law enforcement report **must be filed by you personally**. Once the report has been filed, obtain a copy of your law enforcement report and send a copy to your IDR fraud specialist.

You will receive from your fraud specialist an Identity Theft Affidavit, pre-populated based on information provided by you; please verify all information, sign in the presence of a notary and have it notarized. Make a copy of the notarized affidavit and send it to your IDR fraud specialist. Keep the original copy in a safe place, for your records.

Immediately notify your fraud specialist should you receive any communications from financial institutions, creditors, collection agencies, law enforcement or any other agency relating to your fraud situation.

ID Resolution will assist you while enrolling in monitoring services that track changes to your identity, credit, and account information. Please keep your IDR fraud specialist updated with any additional communications you receive.





# Your Process for Identity recovery

- **Make Copies of Documents**
- **KEEP the Originals!**

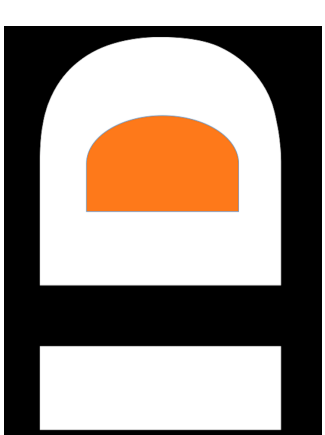
Please photocopy the following identification documents listed below. Send copies to your fraud specialist. These documents will be used in conjunction with letters we create to dispute your fraud.

- Law enforcement report
- Driver's license
- Birth certificate
- Passport
- Social Security Card
- Death Certificate
- Most recent earnings statement from the Social Security Administration
- Previous 3 months of gas, electricity and phone bills.

Also, please send us copies of any letters, statements or documents pertaining to your fraud situation as they are needed to review and resolve your case.

Please do **not** send originals; always keep these in your possession. Only send us legible copies of any documents.

Remember, having filed the law enforcement report and sending your fraud specialist copies of the documents previously mentioned in a timely manner will expedite the fraud resolution process.



# Your Process for Identity recovery

## PII Monitoring

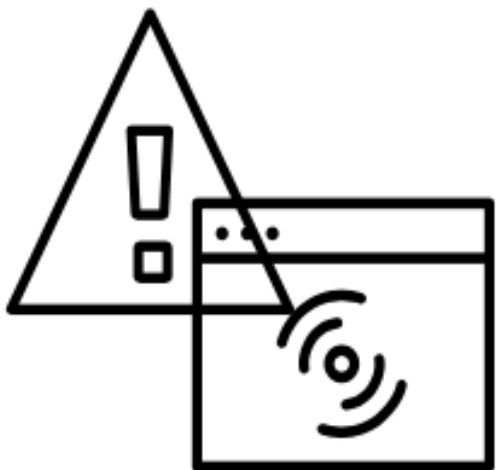
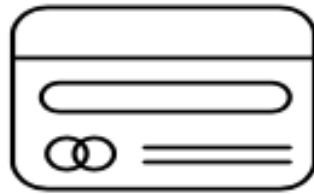
As a victim, we provide you with a whole suite of monitoring tools to monitor your Personally Identifiable Information that may be out there and subject to misuse. Your fraud advocate can discuss it with you in more detail but it includes:



Triple Bureau credit report



Cyber Monitoring of Credit Cards, Bank Accounts, Medical ID, Drivers License etc



Triple Bureau credit monitoring



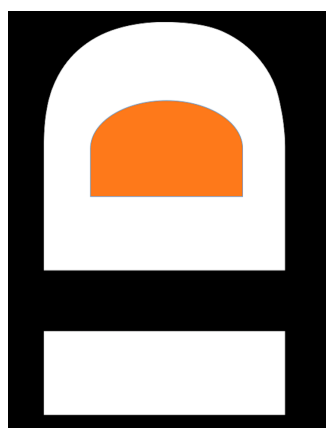
Social Security Number trace



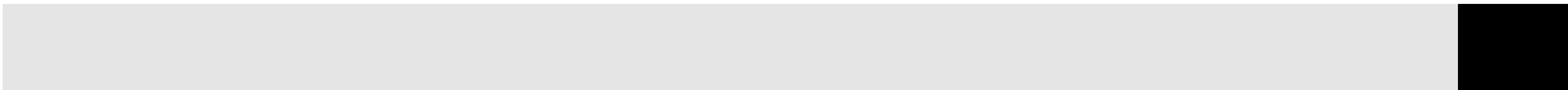
Court Records monitoring



Pay Day Loan Monitoring





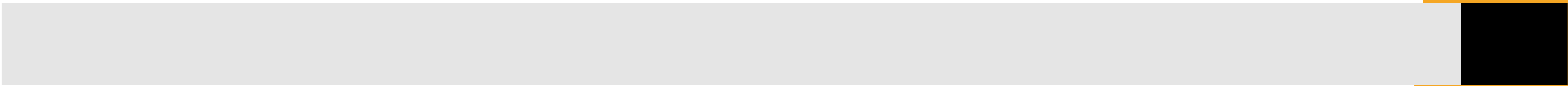
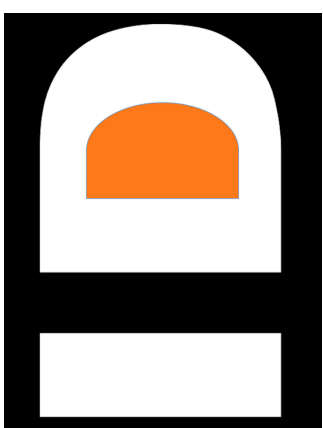


# Your Process for Identity recovery

## PII Monitoring

Other services we can help with include:

	Infant and Minor Identity Risk mitigation. If you have children under the age of 18 we can find out if they have a credit file (they shouldn't !) and make sure they are flagged as minors. Child identity theft is a very real issue.		Unfortunately, every year 3 million deceased have their identities stolen. If you have a bereavement in the family, call us and we'll help protect against identity fraud.
	Personal Document Replacement Assistance - An advocate will assist in replacing sensitive personal identity documents, financial records, legal documents and other critical records..		Relocation of Residence - An advocate can provide guidance on change of address notifications, mail forwarding or bundling, guidance on securing sensitive information during the move, replacement of lost documents, and an Identity Wellness Checkup after the move.
	Identity Travel Response – An advocate will work with governmental agencies to help the traveler get lost documents reissued, work with airlines and hotels to replace lost tickets, interact with local law enforcement, and assist in getting credit cards protected and replaced.		Deployed Military Personnel Identity Risk Mitigation - An advocate can work with family members to review credit and personal information, add a protective Active Duty Military Alert on credit files, and remove names from pre-approved credit offers and personalized marketing for two years.





# Your Process for Identity recovery

## Fraud Alerts versus Credit monitoring

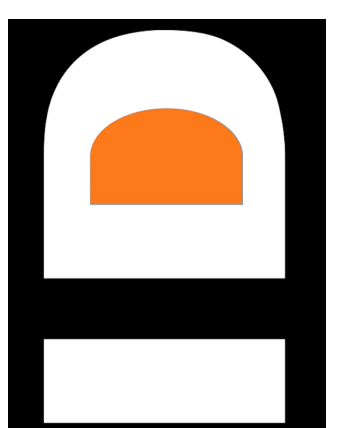
You and your fraud specialist will determine which course of action best suits you and your fraud situation. Your fraud specialist will discuss the pros and cons of each and assist you in the setup process, regardless of your choice.

Fraud Alert (also known as a Security Alert): is a statement placed on your credit file by the three major national credit bureaus; Equifax, Experian and TransUnion.

The alert advises creditors you may be a victim of fraud and to take precautions before extending credit. Most alerts remain in place for 90 days but can be either extended or revoked at any time with the proper documentation. When a fraud alert is added to your credit file, you are entitled to a free credit report from each bureau without utilizing your free annual credit report, mandated by the federal government once a year. NOTE: Credit bureaus are responsible for placing the statement on your credit file, not contacting you if an attempt is made; that responsibility falls on the creditor.

- Pros—No computer or Internet access is required to place the fraud alert. Credit grantors will see the alert when they access your credit report along with your contact numbers, if you choose to leave them. Entitled to a free credit report from each bureau without having to use your free annual credit report, mandated by the FACT Act.

- Cons—An alert may slow or hinder any type of credit or services requiring a credit check (i.e. lines of credit, cell phones or utilities). It is not the alert itself that causes these delays or denials, rather it is the creditor's policy and procedures or systems that they are using. It is optional for the credit grantor to contact you, even though the majority will do so, they are not required.

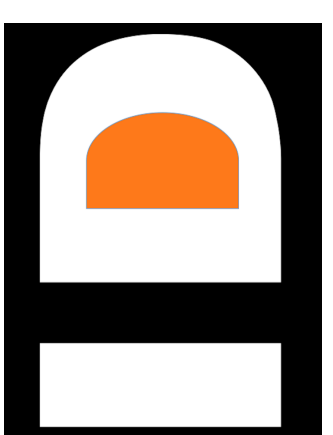




# Your Process for Identity recovery

## Can I do Both? Credit Monitoring and Place Fraud Alerts?

Yes, you can simultaneously have credit monitoring and a fraud alert. However, you may want credit monitoring prior to a fraud alert being placed on your credit file. If a fraud alert is already on your credit file, when you set up your credit monitoring, you may have to go through more rigorous authentication and be asked to verify your identity by phone. The verification questions used to set up your credit monitoring are pulled from your credit report.





# Building a Case File

- **Calendar Of Events**
- **Proof of Fraud**
- **Law Enforcement Documents**

Your fraud specialist will build a managed case file, comprised of information we gather from you, creditors, or other agencies. We advise you to maintain your own case file documentation and any correspondence related to your case. Your case file should be maintained with the most current and accurate information.

## **Retain a chronological calendar of events**

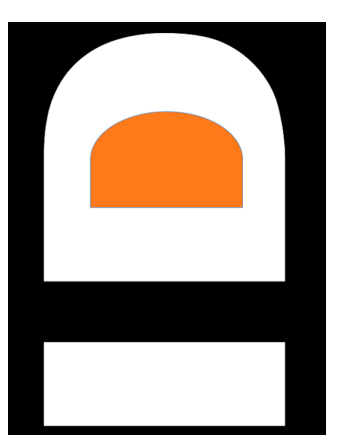
Document all discoveries that will help recapture financial losses. Begin with the original crime and follow through to all subsequent actions. Be sure you log by date: who you spoke to, what was said, all follow-up conversations and dates, fax numbers, email, and mailing addresses. Keep telephone records, court documentation and credit reports. Track changes to your personal profile.

## **Physical proof of fraud**

Keep all applications, credit slips, credit reports, statements and documents that pertain to the fraud. Be time sensitive and report new activity and pertinent documentation.

## **Your law enforcement report and court docket number**

This is your highest priority in the documentation process. Request a copy of your law enforcement report. If that isn't possible, you should request a letter from the detective working the case that he or she cannot provide a physical copy. A case number is not sufficient, although you may have to settle for it. If a fraudster is apprehended and charges are brought against them, keep track of the docket number for this number can change as it moves through the court system.







## Other Directions You Should Follow

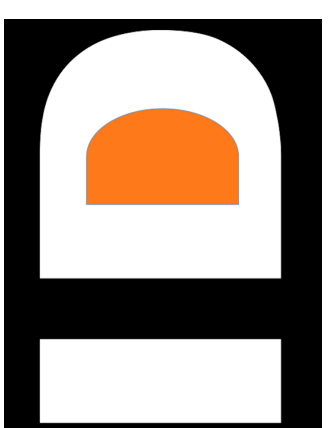
- **Credit Accounts**
- **Debt Collectors**
- **Bank Accounts**

Based on your situation, your fraud specialist will assist you in every area. However, issues may arise before you contact us therefore we have listed some general tips to assist you until you are able to contact us for assistance.

If your credit accounts have been used fraudulently, close these accounts and request new cards to be issued. Have the creditor process these accounts as “accounts closed at consumer’s request due to lost or stolen.” Have the creditor review recent charges and document the dates, dollar amount and to whom the fraudulent charges were made. Ensure that you place any fraudulent charges into dispute or have marked as fraud. Passwords should be created or changed for added security.

Debt collectors may contact you about unpaid bills on fraudulent credit accounts. If this happens, **do not** give out your Social Security Number. You should ask for the person’s name, company name, address and phone number who should then be informed that you are a victim of fraud and not responsible for the account. Obtain information regarding the fraudulent account, such as: original account number, date when account was opened, charges, and if the address differs from yours. A confirmation in writing, along with a completed affidavit of fraud may be needed to confirm that you do not owe the debt and that the account is fraud. Your fraud specialist will do this for you.

We recommend cancelling all checking and savings accounts and obtaining new account numbers. Be aware if you have direct deposit or automatic withdrawals closing your accounts can cause payment delinquencies or other serious issues. However, the banks can open a new account and secure your compromise account to make a smoother transition. It is also prudent to have the bank incorporate an additional password to your account. Ask your bank if they will notify the appropriate check verification companies, such as Scan, ChexSystem and TeleCheck.







# How Did I Become a Victim?

- **Hacking/Data Breach**
- **Mail Theft**
- **"Insider" Compromise**

We may never discover how this occurred but we will have a pretty good idea once the investigation starts. To give you a better understanding, let's identify the ways your personal information can be compromised.

Identity theft is when someone steals your personal information and uses it to commit fraud. They might access your bank accounts to steal money or open new accounts in your name. They might gain employment, buy a car, apply for a loan, all in your name; they are capable of using your identity in any way that they can for illegal financial gains. They might also use your identity to receive health insurance benefits, which could jeopardize your medical records. They will infiltrate anywhere personal information is stored.

## **Computer Hacking**

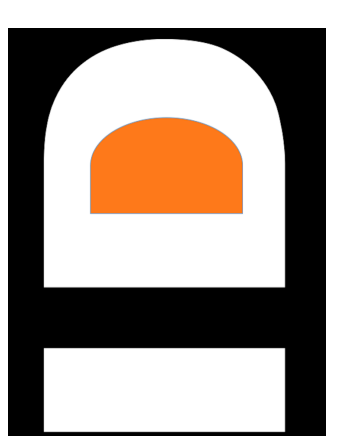
Data stored on your computer or sent from your computer is vulnerable. Beware of potential viruses and put safeguards on your computer. Any entity you have done business with may have stored your personal information electronically, exposing you to the risk of a security breach.

## **Stolen Mail and Documents**

Thieves love this, so shred, shred, shred. Any statement, report, bill, pre-approved credit card or document that divulges your personal information could be enough for an identity thief. They might go through your garbage, dumpsters or unlocked mailboxes to get it. Shred old credit cards, receipts, utility bills, bank statements and any information making you susceptible to fraud.

## **Stealing information from the inside**

This involves accessing businesses that internally store personal data. Identity thieves infiltrate the workplace or imbed accomplices within a business with the sole purpose of stealing identities. Family members can also be perpetrators if they have access to your info such as passwords and PIN codes





# How Did I Become a Victim?

- **Imposters**
- **Medical ID Theft**
- **Financial ID Theft**

## **Imposters**

Thieves will pose as loan officers, charity workers or any position that enables them to obtain vital information from you, either on the phone, by computer or in person.

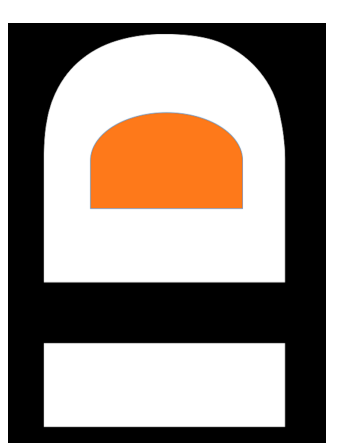
They only need to steal a few pieces of your identity to create havoc with your credit, reputation and financial wellbeing. Thieves set up accounts with new addresses and the more they open successfully with the new address, the more they take control of your identity. They may also steal your identity with the view to getting medical attention and benefits in your name.

## **Financial identity theft**

This variant occurs when a criminal steals your personal information, including any or all of the following: Social Security number; drivers license; passport; home address; mother's maiden name; bank PIN numbers; date of birth; credit cards (or credit card information); and/or personal phone numbers. Thieves use this information to either steal from your existing accounts or make purchases for themselves. They can create new accounts in your name that they control for fraudulent means. This may last for extended periods of time before you are aware to repair the damage. We will discuss preemptive ways of protecting yourself later.

## **Medical identity theft**

This insidious form of fraud occurs when a criminal will steal your personal information and use it to obtain medical services. They will use your identity and insurance to seek medical attention, have expensive operations or, give birth — leaving the bill in your name. In doing so, they will have to changed your vital medical information (blood type, allergic reactions etc.) which can be potentially fatal to you. Always review your Explanation of Benefits (EOB) provided by your insurance company.







# Your Social Security Number is Gold!

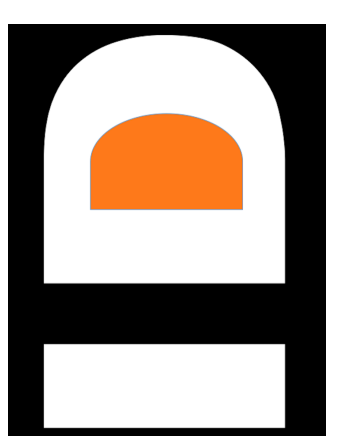
- 
- **Your SSN is Vital. Protect it!**

It should go without saying BUT a Social Security number is the biggest prize to an identity thief. It unlocks bank accounts, credit cards and the rest of your fiscal being.

There are only limited circumstances justifying surrendering this information to someone; government tax agencies, banking and financial institutions would be appropriate examples.

Avoid giving your Social Security number on initial job applications, health provider offices (use the medical ID number off of your insurance card), or over the Internet.

Avoid carrying anything displaying your Social Security number. Most cards no longer detail SSN information to protect you and your identity.





# Lost Official Identification Documents

- **Drivers license**
- **Passport**
- **ATM Debit card**
- **Social Security Number**
- **Mailing Address**

If identifying documents have been lost or stolen, your fraud specialist will assist you with replacing these documents.

## Drivers License

If this is stolen, you should call your state's Department of Motor Vehicles and ask if another license has been issued in your name. When you fill out the appropriate forms to replace your license, please be sure to mark it as lost or stolen. Under certain circumstances, you are able to request a new driver's license number if someone is using yours as identification for cashing forged or stolen checks or using it to commit criminal identity theft. Your ID Resolution fraud specialist can assist with this process.

## Passport

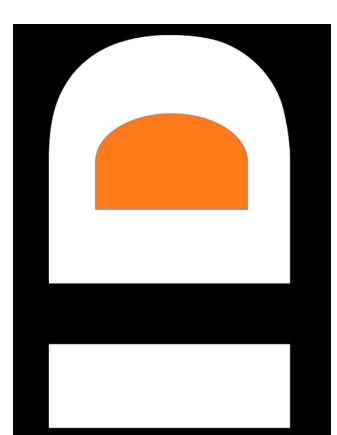
Except in rare circumstances, recent changes mean that Passport renewals/losses are reported and made online. Your fraud specialist can help direct you with this.

## Your Social Security Number

You and your fraud specialist can order and review your Social Security statement. Fraudulent use of your Social Security number might include claiming welfare, benefit fraud or fraudulent employment. The Social Security Administration (SSA) should only be contacted under circumstances of fraudulent use as the agency does not handle cases of financial or criminal identity theft. In rare cases, the SSA will issue you a new number, however, they are averse to doing so.

## Your mailing address

If a thief has filed a change of address with the US Postal Service on your behalf or is using your mailing address to commit fraud, the local postal inspector should be notified immediately. If you and your fraud specialist discover that fraudulent credit cards were sent to a change of address, that local postmaster will need to be alerted and asked to forward all mail in your name to your own address. It also might be beneficial to talk to your own mail carrier. You can also do this online.





# How Can I Keep Myself Safer?

- **Free Credit Reports**
- **Your Wallet**
- **Online Shopping**
- **Social media**
- **Your Computer and Smartphone**

We need to be more mindful than ever to take precautions with our information and to regularly monitor our online activities.

The federal FACT Act of 2003 entitles anyone to get a free credit report once a year from the three credit bureaus, which you should examine carefully for fraudulent activity.

To obtain your free annual credit report, either order online via [www.annualcreditreport.com](http://www.annualcreditreport.com), or by telephone at (877) 322-8228.

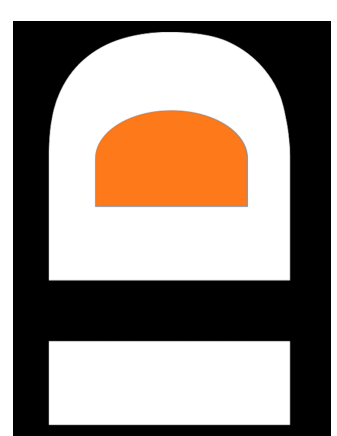
For a copy of the mail-in form, go to:  
<https://www.annualcreditreport.com/cra/requestformfinal.pdf>.

**Avoid carrying personal information, if possible.** Only carry the essential cards for everyday use. Wallets and pocket books are prime targets and their contents will make you vulnerable to identity theft if stolen. Do not leave in your vehicle and keep them safe at work and when travelling.

**Keep your computer safe** — we live in a world of viruses and hackers, so never open up unusual email from unknown sources. Install virus protection software, which will help protect from worms and viruses. Install a firewall to help stop hackers from stealing personal data. All stored data should be encrypted and password protected. When the time comes to dispose of your old computer, use software that securely wipes your hard drive, do not rely on the delete function to remove sensitive information.

When using the Internet for purchases be very conscious of the websites you are using. Be sure they are using secure data transmission and implement strong security and privacy policies.

Make sure you enable passwords and PIN's in your smartphone, keep software up to date and be mindful of whats stored on there. Back up everything regularly!!





# How Can I Keep Myself Safer?

- **Personal Mail**
- **Personal Documents**
- **Passwords**
- **Personal Checks**
- **Credit Cards**

Keep your mail safe- many people now use commercial mail- boxes or P.O. mailboxes to safeguard their mail, on an everyday basis, even when away for extended periods of time.

**Keep and store sensitive information securely**, especially if you have roommates, employ outside help or you are having work done by outside contractors. Make copies of all accounts with expiration dates and customer service phone numbers and store securely, so you are ready for immediate action if the cards are lost or stolen.

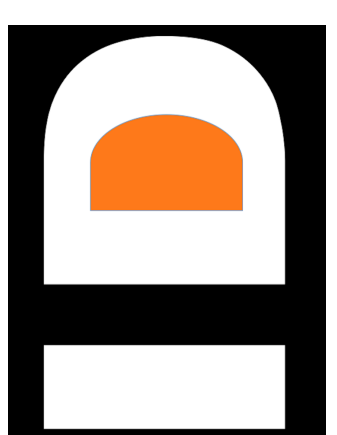
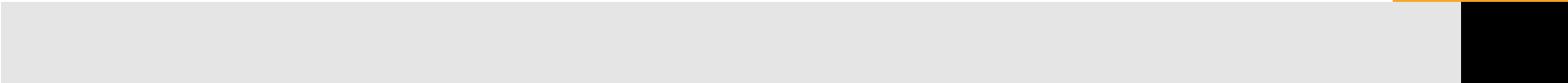
**Check all statements thoroughly for improper use**, including Social Security, phone, bank accounts and credit card statements. Your Social Security statement is mailed about 3 months before the birthday.

**Keep passwords and PINs safe** — passwords to accounts should be alphanumeric (combination of letters and numbers). Thieves are looking for the easily guessed names and numbers. Children's, mother's maiden and pet names are predictable so avoid them. Easily guessed pass codes should be avoided, the last four digits of your Social Security number or birthdays, avoid using those. Create unusual passwords and keep a record of them in a safe place but never carry them with you. Set up additional passwords and security where allowed.

**Keep your checks safe** — mail payments inside post offices. Don't use drop boxes at work or your own mailbox for pick up. Stolen checks can be altered and cashed. Pick up your new checks from the bank, instead of having them mailed, and store-cancelled checks in a safe place.

**Keep the number of credit cards to a minimum.**

Cancelling credit cards can negatively affect credit scores, but keeping unused accounts gives another potential target to identity thieves. Track new or reissued cards that have been sent to you, contact the issuer if the card does not show up in two weeks.







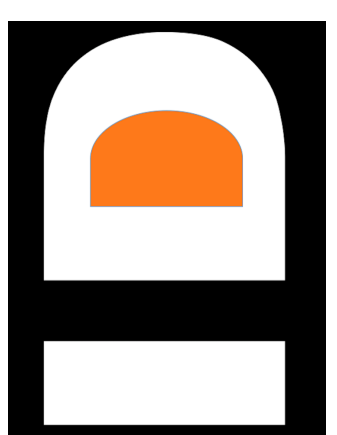
# Unrequested Marketing and Do Not Call

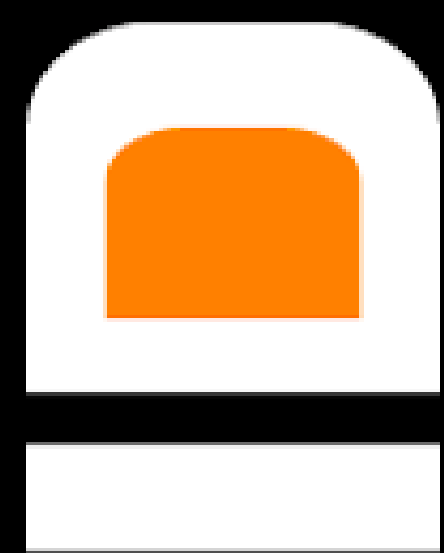
- **If you Don't Want it Act upon It!**

**Stop unrequested marketing** — there are many steps you can take to stop the annoying and unsafe marketing that you may encounter.

Call 1-888-5-optout to have the three credit bureaus remove your name from marketing lists permanently; this will limit the pre-approved credit offers you receive that can be used to obtain fraudulent credit cards in your name.

You can also visit [www.donotcall.gov](http://www.donotcall.gov) or call 888 -382-1222 and they will put your name on the National Do-Not-Call Registry. You can call your State office and add your name to the Do-Not-Call list, if they have one. Never allow any of your financial information to be shared with other financial institutions, credit card companies, insurance or investment firms.





**resolution**

your identity at risk, our solutions at work™

**Contact us:**

[www.idresolution.net](http://www.idresolution.net)