What is identity theft?

You might hear stories on the news about stolen identities, but what is identity theft? When someone uses the personal information that identifies you, like your name, credit card number, or Social Security number to commit crimes like fraud, you have experienced what is identity theft. According to the Federal Trade Commission, 1 in 10 Americans, or 10 million people, learn the hard answer to the question what is identity theft firsthand. You or a friend, relative, co-worker, or acquaintance may have been the victim of identity theft. Renting properties, obtaining credit cards, and purchasing cell phone plans are just some of the transactions identity thieves may make under your name. You might not even realize that your identity has been stolen until it's too late–when you see your soaring credit card bill, your damaged credit score, or the debt collectors come knocking. Knowing what is identity theft can help you stay vigilant.
Although it has been the subject of silly television and movie storylines, as anyone who has found what identity theft is can tell you, it is no laughing matter. Sometimes victims of identity theft are able to fix issues swiftly, but others spend a lot of time and money repairing their credit after seeing what is identity theft. Victims can miss out on job opportunities and get refused educational, automobile, or housing loans due to their damaged credit scores. And they could even be wrongfully arrested for crimes committed by the identity thefts! What is identity theft? It' s something that can happen to any of us, so it is important to be educated on identity theft.

I know what is identity theft–but how do I know if mine has been stolen?

Now that you know the answer to what is identity theft, you should check your credit card accounts and bank statements every month and monitor your credit report regularly. This will help you notice any charges you did not make or incorrect information, which could indicate that your identity has been stolen.
The following situations are also a sign that you have been targeted by identity thieves:

- You are contacted by bill collection agencies for debts that you did not incur.
- A mortgage or car loan you apply for is held up by issues with your credit history.
- You receive strange mail about an apartment you didn't rent, a house you didn't buy, or a job you've never had.

How long can I be affected by identity theft?

Though you may know what is identity theft, you can't really predict how long the effects of identity theft will last. It depends on what kind of theft you've experienced, if the thief sold your information or passed it on to another criminal, if your identity thief is caught, and issues related to fixing your credit report.
Identity theft victims should check their financial reports, like credit card and bank statements, on a monthly basis, and their credit reports every three months in the first year, then once a year after that.
If you know firsthand what is identity theft, do not delay: take the steps to correct your financial

records and contact companies that allowed fraudulent accounts. Call first, then follow up in writing.

How do thieves commit identity theft?

Thieves know what is identity theft and they're adept at getting your personal information. Here are some of the ways they may target you:

Dumpster diving.

If you toss your mail without worrying about thieves, you may learn what is identity theft the hard way. Thieves root through garbage to find bills, pre-approved credit offers, and other papers full of your personal details. Thwart them by shredding all documents before trashing or recycling them.

Skimming.

An identity thief could work in a store or restaurant–they'll steal your credit and debit numbers during legitimate transactions using special technology. Monitor your statements to catch them.

Phishing.

Thieves can masquerade as companies or financial institutions, sending you spam emails to trick you into divulging information. Never give out personal information online unless it is a verified transaction, lest you know what is identity theft through personal experience.

Changing your address.

A thief might change your address, sending your statements to an alternate location that allows them to get your information. Take note if you do not receive your bills or bank statements and inquire with the post office, or move to paperless statements and avoid the truth of what is identity theft!

Old-fashioned stealing.

Wallets, purses, mail, pre-approved credit offers, new checks or tax information–all of these items can be stolen by identity thieves to aid their cause. Be careful with your personal items in public, and check your mail frequently.

Pretexting.

Identity thieves might even target financial institutions or other companies that have your personal information, using false pretenses to gain access. Make it more difficult for them by having different passwords for all of your accounts.

How do thieves use a stolen identity?

To fully understand what is identity theft, you should know how thieves may use a stolen identity:

Credit card fraud.

Thieves open new credit cards under your name, use them however they please, and let the bills build up. Debts incurred end up on your credit report. Or they'll change your billing address on an existing card so that you never see your bills, allowing them to make purchases you won't notice.

Phone or utilities fraud.

Like with credit card fraud, identity thieves can open a new landline or wireless account in your name, or charge up an existing account by changing your address. They'll also use your name

and information to get their own electricity, heating, or even cable television.

Bank or finance fraud.

Using your name or account number, thieves can create and use fake checks. They can also open a new account under your name to write bad checks, copy an existing ATM or debit card to make withdrawals online, or get a loan for themselves under your name!

Government documents fraud.

Thieves can even fool the government. They'll get an official picture ID, like a driver's license, issued under your name. They'll use your Social Security number and name to receive government benefits. They'll file fake tax returns using your information, making you criminally liable.

Other fraud.

What is identity theft? It also encompasses other fraud committed under your name. Thieves can get jobs under your Social Security number, rent properties under your name, seek medical treatment with your information, or even give out your information when they're arrested, creating an arrest warrant under your name if they don't show up for court!

Fighting identity theft

Avoid finding out what is identity theft firsthand with R&R Financial Group!Call us at (708) 680-7600.

What is an Identity Theft Report?

In a way, an Identity Theft Report is like a police report that includes extensive details about how the identity thieves used your information. When your identity is stolen, you will give the police and the government information about the crimes committed against you, and they compile this information into your Identity Theft Report. They make the Identity Theft Report so detailed so that the credit reporting companies and businesses can verify that you are a victim and recognize which information and accounts on your credit report are false. Whereas regular police reports don't go into detail about the accounts identity thieves open or abuse, an Identity Theft Report highlights them.

When you realize that you are a victim of identity theft, you will file an ID Theft Complaint Form with the Federal Trade Commission, or FTC. The police can use a printed copy of this form to furnish their police report with additional information, but they are not legally required to do so, as they may have alternate means to include detailed information about the crime in their own reports. If the police report is detailed enough, it can stand in for the the Identity Theft Report.

How to Create & Use an Identity Theft Report
Step 1: File Your Identity Theft Report

You will file your Identity Theft Report with a local, state, or federal law enforcement agency. These might include your city police department, the State Attorney General, the Federal Bureau of Investigation, the U.S. Secret Service, the FTC, or even the U.S. Postal Inspection Service. There are some state laws requiring local police departments to make an Identity Theft Report, but no federal agencies are required to take them.

In the Identity Theft Report, you must provide the most information you can. This includes any

information on the fraudulent accounts that were opened, the dates of the identity theft, and the alleged identity thief. By filing your ID Theft Complaint Form with the FTC, then furnishing this completed form to the local law enforcement, you can help ensure that the Identity Theft Report is thorough enough. The police officer or other law enforcement agent can either attach your ID Theft Complaint Form to the police report or incorporate the information into their report.
Once the police report is completed, as the officer for a copy of the official Identity Theft Report. Sometimes the officer will not be able to do so, but they can sign a copy of the ID Theft Complaint Form and write the official police report number in the "Law Enforcement Report" section of the ID Theft Complaint Form.
Be aware that there is no legal requirement for the police to use the ID Theft Complaint Form in their report. They may have an alternate way to include details of the identity theft in the Identity Theft Report, and in this case, the police report will serve as the Identity Theft Report.
Since a detailed Identity Theft Report is necessary for you to get certain protections on your credit, you might consider enclosing a cover letter explaining how important it is for your Identity Theft Report to be detailed. Work with the police and give them as much information as possible.

Step 2: Send Out Your Identity Theft Report

Next, you should send your Identity Theft Report to the credit reporting agencies as well as the businesses involved in your identity theft. Be sure to include a cover letter when sending your Identity Theft Report to the three credit reporting agencies, plus any documentation that gives more information on your identity theft. When you send your Identity Theft Report to the fraud departments of the businesses where your identity thief committed fraud with your personal information, also enclose supporting documentation and a cover letter that details whether fraud was committed on an existing account or on a new account opened by the thief. Whether you are sending your Identity Theft Report to the credit reporting companies or a business' fraud department, send the Identity Theft Report by certified mail and request a return receipt.
If your Identity Theft Report does not have enough detailed information for the companies or credit reporting agencies to determine that you are a victim of identity theft, they will decline your Identity Theft Report. If this happens, they will let you know that your Identity Theft Report needs more information within 15 days of receiving it. The business or credit reporting agency then has 15 additional days to collaborate with you and ensure that your Identity Theft Report contains all the information they need. Once they receive additional documentation and information, they have 5 more days to review it before making a decision.

How You Can Use Your Identity Theft Report

Why should you go through the process of creating and sending an Identity Theft Report? You can use your Identity Theft Report in many ways to protect your credit, including:
Removing fraudulent details from your credit report–and ensuring that they don't appear again. The credit reporting companies prevent false information from marring your credit report after you file your Identity Theft Report with them. If you properly file your Identity Theft Report with the businesses where the thief used your information as well as the credit reporting companies, it will keep the thieves' debts from appearing on your credit report now and in the

future.
Stop collections on fraudulent debts. The Identity Theft Report can also stop a business from trying to collect debts the identity thieves incurred or selling those debts to collection agencies.
Place an extended fraud alert on your credit report. Submitting your Identity Theft Report will place a fraud alert on your account so that creditors will have to contact you by phone or in person to confirm your identity and that you are applying for credit in your name. This alert will remain on your credit report for 7 years.

What To Do If Your Identity Was Stolen

Filing a police report, checking your credit reports, notifying creditors, and disputing any unauthorized transactions are some of the steps you must take immediately to restore your good name. To file a complaint, contact the FTC.

How do I prove that I'm an identity theft victim?

Applications or other transaction records related to the theft of your identity may help you prove that you are a victim. For example, you may be able to show that the signature on an application is not yours. These documents also may contain information about the identity thief that is valuable to law enforcement. By law, companies must give you a copy of the application or other business transaction records relating to your identity theft if you submit your request in writing, accompanied by a police report.

Should you file a police report if your identity is stolen?

A police report that provides specific details of the identity theft is considered an Identity Theft Report, which entitles you to certain legal rights when it is provided to the three major credit reporting agencies or to companies where the thief misused your information. An Identity Theft Report can be used to permanently block fraudulent information that results from identity theft, such as accounts or addresses, from appearing on your credit report. It will also make sure these debts do not reappear on your credit reports. Identity Theft Reports can prevent a company from continuing to collect debts that result from identity theft, or selling them to others for collection. An Identity Theft Report is also needed to place an extended fraud alert on your credit report. You may not need an Identity Theft Report if the thief made charges on an existing account and you have been able to work with the company to resolve the dispute. Where an identity thief has opened new accounts in your name, or where fraudulent charges have been reported to the consumer reporting agencies, you should obtain an Identity Theft Report so that you can take advantage of the protections you are entitled to.
In order for a police report to entitle you to the legal rights mentioned above, it must contain specific details about the identity theft. You should file an ID Theft Complaint with the FTC and bring your printed ID Theft Complaint with you to the police station when you file your police report. The printed ID Theft Complaint can be used to support your local police report to ensure that it includes the detail required.
A police report is also needed to get copies of the thief's application, as well as transaction

information from companies that dealt with the thief. To get this information, you must submit a request in writing.

What do I do if the local police won't take a report?

There are efforts at the federal, state and local level to ensure that local law enforcement agencies understand identity theft, its impact on victims, and the importance of taking a police report. However, we still hear that some departments are not taking reports. The following tips may help you to get a report if you're having difficulties:

Provide the officer with a copy of the "Law Enforcement Cover Letter" that explains why the police report and the Identity Theft Report are so important to both victims and industry.

Furnish as much documentation as you can to prove your case. Debt collection letters, credit reports, a copy of your printed ID Theft Complaint, and other evidence of fraudulent activity can help demonstrate the legitimacy of your case. Provide the police a copy of "Remedying the Effects of Identity Theft," which shows that police reports are necessary to secure your rights.

Be persistent if local authorities tell you that they can't take a report. Stress the importance of a police report; many creditors require one to resolve your dispute. Remind them that consumer reporting companies will automatically block the fraudulent accounts and bad debts from appearing on your credit report, but only if you can give them a copy of the police report. In addition, a police report may be needed to obtain the fraudulent application and other records the company has.

If you're told that identity theft is not a crime under your state law, ask to file a Miscellaneous Incident Report instead.

If you can't get the local police to take a report, try your county police. If that doesn't work, try your state police.

Some states require the police to take reports for identity theft. Check with the office of your State Attorney General, which can be found at www.naag.org, to find out if your state has this law.

What do I do if the police only take identity theft reports over the phone?

The FTC ID Theft Complaint has a special section for police reports that are not filed face-to-face, to help you use it to supplement an automated police report. If you file a police report online or over the phone, complete the "Automated Report Information" block of the ID Theft Complaint. Attach a copy of any filing confirmation received from the police.

If you have a choice, however, you should file your police report in person and not use an automated report. It is more difficult for the consumer reporting company and information provider to verify the information in an automated report, and they will likely require additional information and/or documentation.

What is a credit freeze?

Many states have laws that let consumers "freeze" their credit – in other words, letting a consumer restrict access to his or her credit report. If you place a credit freeze, potential creditors

and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. This means that it's unlikely that an identity thief would be able to open a new account in your name. Placing a credit freeze does not affect your credit score – nor does it keep you from getting your free annual credit report, or from buying your credit report or score. Credit freeze laws vary from state to state. In some states, anyone can freeze their credit file, while in other states, only identity theft victims can. The cost of placing, temporarily lifting, and removing a credit freeze also varies. Many states make credit freezes free for identity theft victims, while other consumers pay a fee – typically $10. It's also important to know that these costs are for each of the credit reporting agencies. If you want to freeze your credit, it would mean placing the freeze with each of three credit reporting agencies, and paying the fee to each one.

What does a credit freeze not do?

While a credit freeze can help keep an identity thief from opening most new accounts in your name, it's not a solution to all types of identity theft. It will not protect you, for example, from an identity thief who uses your existing credit cards or other accounts. There are also new accounts, such as telephone, wireless, and bank accounts, which an ID thief could open without a credit check. In addition, some creditors might open an account without first getting your credit report. And, if there's identity theft already going on when you place the credit freeze, the freeze itself won't be able to stop it. While a credit freeze may not protect you in these kinds of cases, it can protect you from the vast majority of identity theft that involves opening a new line of credit.

Who can access my credit report if I place a credit freeze?

If you place a credit freeze, you will continue to have access to your free annual credit report. You'll also be able to buy your credit report and credit score even after placing a credit freeze. Companies that you do business with will still have access to your credit report – for example, your mortgage, credit card, or cell phone company – as would collection agencies that are working for one of those companies. Companies will also still be able to offer you prescreened credit. Those are the credit offers you receive in the mail that you have not applied for. Additionally, in some states, potential employers, insurance companies, landlords, and other non-creditors can still get access to your credit report with a credit freeze in place.

Can I temporarily lift my credit freeze if I need to let someone check my credit report?

If you want to apply for a loan or credit card, or otherwise need to give someone access to your credit report and that person is not covered by an exception to the credit freeze law, you would need to temporarily lift the credit freeze. You would do that by using a PIN that each credit reporting agency would send once you placed the credit freeze. In most states, you'd have to pay a fee to lift the credit freeze. Most states currently give the credit reporting agencies three days to lift the credit freeze. This might keep you from getting "instant" credit, which may be something to weigh when considering a credit freeze.

What is a fraud alert?

There are two types of fraud alerts: an initial alert, and an extended alert.
An initial fraud alert stays on your credit report for at least 90 days. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial alert is appropriate if your wallet has been stolen or if you've been taken in by a "phishing" scam. With an initial fraud alert, potential creditors must use what the law refers to as "reasonable policies and procedures" to verify your identity before issuing credit in your name. However, the steps potential creditors take to verify your identity may not always alert them that the applicant is not you. When you place an initial fraud alert on your credit report, you're entitled to order one free credit report from each of the three nationwide consumer reporting companies, and, if you ask, only the last four digits of your Social Security number will appear on your credit reports.
An extended fraud alert stays on your credit report for seven years. You can have an extended alert placed on your credit report if you've been a victim of identity theft and you provide the consumer reporting company with an Identity Theft Report. An automated Identity Theft Report should be sufficient to obtain an extended fraud alert. With an extended fraud alert, potential creditors must actually contact you, or meet with you in person, before they issue you credit. When you place an extended alert on your credit report, you're entitled to two free credit reports within twelve months from each of the three nationwide consumer reporting companies. In addition, the consumer reporting companies will remove your name from marketing lists for pre-screened credit offers for five years unless you ask them to put your name back on the list before then.
To place either of these alerts on your credit report, or to have them removed, you will be required to provide appropriate proof of your identity: that may include your Social Security number, name, address and other personal information requested by the consumer reporting company.
As mentioned, depending on the type of fraud alert you place, potential creditors must either contact you or take reasonable steps to verify your identity. This may cause some delays if you're trying to obtain credit. To compensate for possible delays, you may wish to include a cell phone number, where you can be reached easily, in your alert. Remember to keep all contact information in your alert current.

What does a fraud alert not do?

While a fraud alert can help keep an identity thief from opening new accounts in your name, it's not a solution to all types of identity theft. It will not protect you from an identity thief using your existing credit cards or other accounts. It also will not protect you from an identity thief opening new accounts in your name that do not require a credit check – such as a telephone, wireless, or bank account. And, if there's identity theft already going on when you place the fraud alert, the fraud alert alone won't stop it. A fraud alert, however, can be extremely useful in stopping identity theft that involves opening a new line of credit.

What's the difference between a credit freeze and a fraud alert?

A fraud alert is another tool for people who've had their ID stolen – or who suspect it may have been stolen. With a fraud alert in place, businesses may still check your credit report. Depending on whether you place an initial 90-day fraud alert or an extended fraud alert, potential creditors must either contact you or use what the law refers to as "reasonable policies and procedures" to verify your identity before issuing credit in your name. However, the steps potential creditors take to verify your identity may not always alert them that the applicant is not you.

A credit freeze, on the other hand, will prevent potential creditors and other third parties from accessing your credit report at all, unless you lift the freeze or already have a relationship with the company. Some consumers use credit freezes because they feel they give more protection. As with credit freezes, fraud alerts are mainly effective against new credit accounts being opened in your name, but will likely not stop thieves from using your existing accounts, or opening new accounts such as new telephone or wireless accounts, where credit is often not checked. Also, only people who've had their ID stolen – or who suspect it may have been stolen, may place fraud alerts. In some states, anyone can place a credit freeze.