

Steps to Take to Protect Yourself if you are a Victim of Identity Theft

Did a thief get their hands on your personal finances? Did someone scam you? Do you see fraudulent activity on any of your accounts? Then you may be a victim of identity theft.

What is identity theft?

Identity theft is ugly. To be a victim of identity theft is really no fun.

Identity theft is when a thief gets access to your personal and financial information. Through dark and mysterious activity, they find ways to break into your personal and financial space. Your SSN, legal name, credit card accounts, bank accounts, tax files, you name it. They make themselves at home and take on your name and details.

Once they carry your identity they can do anything in your name. They may deplete your bank accounts of its funds. Thieves may apply for new credit lines, rack up balances, and leave you with the balances. They may steal your tax refunds, or better yet, file fraudulent tax returns.

Wherever they can pull dollars from, they will. All in your name. That can be devastating to your financial status in every way. Be it due to debt they leave you with, the effects of damage to your criminal records, or simply the money it takes to clean up an identity theft mess.

Can you Protect Yourself from Identity Theft?

Just to think of what it is like to be a victim of identity theft is enough to make you shudder.

If it happened to you, there are several steps you can take to protect yourself further. Even if someone stole your identity, you don't have to let them walk away with more than you can prevent. That said, there are several types of identity theft. For each one, I will advise what you can do to protect yourself further.

Let me warn you upfront. It is a headache. Protecting yourself against identity theft requires lots of paperwork. It requires you to speak up quickly. You may need to fight for refunds. I hope this post will make the process as smooth as possible. And rest assured, you will make it through.

First file a police report

Before you do anything, first file a police report. Or as it may be called, a fraud affidavit.

That is an absolute must for step 1. This report is to prove to all that you are a victim of identity theft. It will make it easier for you to fight the fraudulent activity if you have this official report. It will also help you restore your losses more easily.

You can file a fraud affidavit online. When you do, fill it out carefully. The information should be as accurate as possible. You want to ensure it goes as smoothly as possible. You don't need extra headaches or delays due to wrong information on your fraud affidavit.

In order to file a fraud affidavit, visit [this link](#). It is on

the Federal Trade Commission website. You will be prompted to click the get started button. Do so and then follow the prompts.

A fraud affidavit gives you the opportunity to report the theft and start the road to recovery. It's important you take this step immediately to make the recovery easier.

Now, we're ready to dive into each identity theft type you may have been a victim of. Read what you can do to protect yourself further.

1. Protect Yourself from Fraudulent Banks Accounts

One thing a hacker may do after they steal your identity is open bank accounts in your name.

They can literally apply for accounts with the banks you bank with. Thieves may open new accounts to use for checks. They can write out a bunch of checks and leave you to deal with bounced check fees. The debt can pile up from account fees.

They also like to use the accounts for criminal activity. If they perform a crime through your bank account then it leaves their personal name out of the crime. But you are left with enormous debt and you are not at all anonymous. The new bank accounts belong to you after all.

The good news is that you are protected under federal regulation for this sort of identity theft. You will not have to swallow the general fees, the overdraft fund fees, or fees for the bounced checks.

Regarding the crime committed through the bank account, we will discuss later if you need to take responsibility for the resulting loss.

So, what can you do to prevent this from happening again?

You can check your bank account activity report.

There are companies that note bank account activity. That includes when you open and close bank accounts. Most banks report to these companies and you can see it all on your bank account activity report. These reports also list if you had bounced checks, overdraft protection, and more.

Federal law mandates that you can get your report once a year for free. Definitely check your report once a year. Look out for new bank accounts that you don't recognize opening. Search for fraudulent activity on your report. If you already are suspicious of fraudulent activity, check your report twice a year. The first time you will get it for free but you should order it a second time for a small fee. It is important to do so to ensure you don't miss fraud if there is.

These are some companies from whom you can order your bank screening reports:

Check your soft inquiries

There is another thing you can do to prevent fraudulent bank accounts in your name.

Many banks do a soft pull on your credit before they open a new account for you. They do it in order to check your credit file before they entrust you with an account.

Banks that offer overdraft protections and similar services are even more likely to check your credit before they choose to grant you an account. Just like an employer interviews a potential employee, the bank wants to scan your credit life before they approve you for a new account.

This can work in your favor if you suspect fraudulent bank

accounts. You can check to see recent soft pulls and look out for fraudulent ones.

A fraudulent inquiry is one from a bank that you know you have not opened an account with. Or if there are multiple from a specific bank you know you don't have so many accounts with.

You can view your soft inquiries on your credit report. You can view your credit report at annualcreditreport.com for free, once every 12 months. Make sure that all inquiries you see are from bank accounts you opened. If there are some you don't recognize, look into it to make sure those are not fraud accounts opened through identity theft.

2. Protect Yourself from Fraudulent Credit Cards

Another popular treat for identity thieves is to open credit lines. This includes credit cards and loans.

They can open these up in your name as soon as they have your personal information. With your social security number, name, address, and date of birth, they can go party and apply for credit lines. The rest of the information they need to apply is simple for them to make up or figure out. That includes facts such as your income and housing expenses.

A thief may open credit cards under your name, swipe thousands of dollars, and then go fly off. You are then left with all that debt to pay up.

Your credit score is also at stake

Not only are you left with debt, but the thief can also subsequently ruin your credit. Following are some aspects of a credit score that can be affected if a thief messes with credit lines in your name.

Too many new accounts opened

Credit scoring models do not like to see so many credit cards opened in one shot. As a matter of fact, each time you open a new card, your score will drop a bit. This is due to a couple of factors.

One reason is that when you apply for a new card, the bank does a hard pull to your credit. This is the act of them accessing your credit report to look it through.

The bank will do this before approving (or declining) you for a card. Whether you get approved or denied the card, a hard inquiry will show up on your credit report. Each hard inquiry will push your credit score down by a few points. That is a general rule. That is because it is bad to have too many recent inquiries. No lender wants to see that you applied for so many new accounts. Why would they trust you to be responsible with yet another credit card after opening so many?

Do you see where we're going with this? Do you think had the thieves realized they were doing this much damage they would have kept away? If only.

Another reason a new account affects your score is this. Automatically, once the new account reports to your credit, your score will drop a bit. The credit models want to see how you will take this new account. Can you handle the new credit line or not? After an approximate period of up to 30 days, your score will go up again. If the thief opens multiple accounts, the effect it has on your credit score will be much stronger. Negatively, that is. Due to the hard credit inquiries and simply for having new accounts.

High credit utilization

This is yet another way identity theft affects your credit.

The thief opens new credit cards, swipes tons of money, and leaves you with unpaid balances. There goes your credit utilization.

Credit utilization is the ratio of the credit limit on your credit card and the card balance. If the balance is high in regards to the available credit, then your credit utilization is high. That is not good. Credit utilization should ideally be low. Even as low as a balance that is only up to 9% of the credit limit on the card.

Seems the thieves didn't know this rule. They likely used a lot more of the available credit on your credit cards.

Credit utilization likely shot up from those balances. And that obviously can cause your credit score to shoot downwards.

Dealing with the debt and sour credit score

This is a two-edged sword. On one end you have credit cards with huge balances, and on the other end, you have blue and black bruised-up credit.

Lucky for you, you do not have to pay the balances. In most states, the law claims you are not responsible for debt on fraudulent accounts that were opened in your name. So that's good. It helps you financially so that you don't have to pay those credit cards.

And about your credit, the Fair Credit Report Act (FCRA) demands that the credit bureaus remove any account from your report that was opened without your consent. But, the damage done to your credit is done. It is difficult to go back on it, even once you remove the accounts.

Here is how you can protect yourself further to ensure no thief touches your credit. It is too demanding to risk it otherwise.

Freeze your credit

First things first, freeze your credit. I'll explain what that means. When you apply for a new credit line, the lender will pull your credit report before they approve you. This, as we mentioned above, is to help them decide if they want to extend credit to you.

Now, you can freeze your credit report. If you log in to your online credit report with any one of the credit bureaus, you can easily place a freeze on your credit. This locks your report and everyone but you loses access to your credit report. So if a thief applies for a card in your name, the bank will try to pull your credit. But if there is a freeze, they will not be able to pull your credit. Thereupon, they will not be able to approve the new card account.

Ha, thief, caught you right there! When you freeze your credit you elegantly keep the thieves' hands off your credit. They will be unable to open new credit lines in your name in such a manner.

According to the FCRA, you have the right to freeze your credit for free whenever you'd like. You can, at any time, freeze or unfreeze your report. So it's not like you're locking yourself in forever. If you need to apply for a new card, you can unfreeze the report for the time being.

Place a fraud alert on your report

Secondly, to protect yourself from fraudulent credit lines, you can place a fraud alert on your credit report. When a lender pulls your credit before they approve you for new credit, they will get a message to be extra cautious. The message may be similar to this: *"Identity security ALERT: Fraudulent applications may be submitted in my name or my identity may have been used without my consent to fraudulently obtain goods or services. Do not extend credit without first*

verifying the identity of the applicant.”

So if a thief is trying to apply for a new credit card, they may be hit with additional security verification steps. The lender may ask for more documents, security questions, and more. The thief will have to work harder to prove your identity and may fail. If the bank cannot confirm your identity, they will not extend the credit. You can call each of the credit bureaus to ask for a fraud alert on your report. You can also contact the credit bureaus online. It is free to place a fraud alert on your credit report.

Please note: If you place a fraud alert, it may give you a hard time to apply for legitimate accounts. The lenders will double down on the security for you as well. After all, they can't prove at the onset if you are the legit applicant or not. So it may be difficult to apply for credit if you have a fraud alert. I therefore would not suggest you put a fraud alert as a first step. Do so only as a last resort, if a credit freeze is not enough.

To remove a fraud alert, you will have to mail a request to all three credit bureaus. You will need to provide identifying documents.

Apply for credit monitoring

You can get alerts from your credit report even more simply with a credit monitoring service. This will not cause complications as a fraud alert may.

There are companies who can monitor your credit report for free. They can alert you of every action that is done on your report. If there is a new inquiry on your report, they will notify you. If the inquiry is not from an account you applied for, you can notify the consequential bank immediately. They will cancel the application and not extend the credit. That's called to nip it in the bud.

When you are alerted before the act is finished, you can make sure the account does not even get opened.

There are many companies that monitor your credit for free. Each one reports from some or all of the credit bureaus. The companies also differ in terms of the frequency in which they update their info. See which one works for you.

Here are a few options:

3. Protect Yourself from Theft with your Credit Card Rewards

There is another dimension to credit card identity theft. That is when thieves break into your online account and steal your credit card rewards. Your hard-earned credit card rewards. Many credit cards offer rewards on certain purchases you make with your credit card. For example, a card may offer 1 point per each dollar spent on office supplies.

The approximate value of a point is 1 cent per point. The rewards you earn can be redeemed as cashback, for travel, and more. It can take time, thought, and money to rack up a significant amount of points. Besides it is upsetting to lose all your rewards, there is nothing to do to protect your points from being stolen.

I'm sorry! If you lose your rewards to identity theft, there is not much you can do. However, do reach out to your credit card lender. Sometimes, you are able to get your rewards back as a courtesy of the bank.

So if you lost rewards from an Amex credit card, reach out to Amex. If you lost Chase points, reach out to Chase, etc.

4. Protect Yourself from Fraudulent Activity in your Bank Accounts

Identity thieves may trample your existing bank accounts. All they need is your checking account number or debit card number. Even simply having the login to your online banking can give them access to your accounts. Once they can access your bank accounts they can easily drain your accounts from the money in it. They can transfer funds out of your accounts and use the funds for whatever they please.

Since that can be devastating, here are some practical ways to protect yourself and prevent this from happening.

Set up alerts

You should have the option with most banks to set up alerts. You can preset which type of activities you want to be alerted of. Activities may be; when a transaction surpasses a certain amount, your personal information such as your address or phone number change, when you get a transfer of funds going in or coming out of your account, and more.

These alerts are great for monitoring fraudulent activity. If you get alerted for something you know wasn't you, you can crack down on it immediately. Call the bank, stop the transaction, whatever it takes to prevent fraud.

Review your bank statements

Always review your bank statements carefully. If you ever suspect fraudulent activity, get in touch with your bank immediately. If there are transactions you don't recognize, make sure to act upon it and let the bank know.

Set strong credentials

This is definitely a must for online accounts. Set a strong password so that it should be harder for thieves to crack in. You can opt for two-step verifications to give them an even harder time. Don't go easy on those identity thieves! These are ideas to prevent identity theft from occurring.

But what if you are already a victim? You can be protected from your loss if you act quickly.

If you contact your bank as soon as possible after you notice fraud, you stand the chance of being protected. With Federal banking regulations, it all depends when you report fraudulent bank transactions. If you report within 2 days of when you receive your statement then you will be protected. There will be a \$50 liability. If you report on the third day then your liability will jump to \$500. If you report transactions past 60 then you will not be protected. That means that you will be protected for transactions that happened within the first 60 days, but not for transactions past 60 days.

You can understand from here that it is crucial to report fraud ASAP when it comes to bank activity. If you wait too long, your liability will increase and you may even risk not being protected at all.

5. Protect Yourself from Fraudulent Activity with your Taxes

There are two things in life that you can't avoid, correct? Death and taxes.

And taxes is a looming headache.

Do you know how you can turn taxes from a headache to a magnified migraine? When you add tax identity theft to the mix.

Identity thieves can hack into your tax files. They may file fraudulent tax returns in your name. Then they may take your tax refund and go home. They can even exaggerate the tax returns for an inflated refund.

Tax identity theft involves many issues. First of all, the thief walks off with tax credits under your name. That means that you either miss out on your legitimate tax refunds or that your refunds get very delayed. That is a monetary loss.

Plus, there is loads of paperwork you have to deal with to sort out the mess. To get your files back in order, correspondence with the IRS, and much more.

The bad news is that if you are a victim, you have to deal with all of the above. Fortunately, though, there are some steps you can take to protect yourself and prevent this from happening again.

File taxes as soon as you can

The IRS will accept the first tax returns that come in for any given person. Make sure you are the first one to file taxes under your name.

You hope to be the only one but in case someone has got their dirty hands on your file, this tactic can save you. File your taxes as soon as you possibly can. Make sure you beat any fraudulent tax returns that may come in under your name.

First come, first serve. This is a matter a lot more crucial than pizza and fries, to ensure you're first in line for!

Get an IP PIN

Another way to protect yourself is to get an IP PIN.

An IP PIN is a six-digit code you can get from the IRS. The IRS usually will assign an IP PIN to any victim of identity

theft.

You may even get one if you are a possible victim.

A new PIN will be generated for you each year. You use the IP PIN when you file taxes to prevent anyone else from filing your taxes.

It's your secret passcode to your tax returns. It is assigned just to you and should stay confidential. Obviously, if you have a tax professional file your taxes you will need to share your PIN but keep it at that. No one but the IRS and the filer need to know your PIN.

You can check this out for every detail you need to know about IP PINs.

6. Protect Yourself from Fraudulent Employment or Unemployment

One thing you may wish for is to have a robot go to work instead of you. Let the machine be the one to wake up early and operate 9-5.

But as long as you get the green bills at the end of the day, huh?

So some thieves will come in and take the cash, but leave you to work. This is known as employment identity theft. Or unemployment identity theft, when they file unemployment for you and cash in on the cash.

Either way, it's nasty. Whether they work under your name and get paid, or file unemployment and get your insurance checks. Luckily, the IRS will bear the brunt of your loss for all things money. But it's a lot to sort out in terms of paperwork and filing.

Here are a few things you can do to investigate and protect

yourself.

Request a wage transcript

Just like you can ask for a bank account activity report, you can ask for a wage transcript.

Ask your accountant to request from the IRS your wage transcript. There you can view all wages under your name. Search for fraudulent wage reports if you suspect identity theft.

Once you review that and come across fraud, these are 3 places you should report to:

1. **Your employer:** Report the fraud to your employer so they know what is going on. Keep copies of all communications.
2. **U.S. Department of Justice's National Center for Disaster Fraud:** Also known as NCDF. You can report your fraud either online here or call 1-866-720-5721.
3. **U.S. Department of Labor:** Report fraudulent unemployment here.

7. Protect Yourself from Fraudulent Criminal Records

This is a tough one, though not that common. Imagine if you have stained criminal records done by some stranger lurking out there.

Identity thieves may actually commit crimes using your information. That equals crime done in your name. Thieves may commit the crime under your name or even give over your personal information, standing in for their own, to a police officer. No one can be the wiser if you were the one to commit the crime or not. It is a tough tangle to crawl out of.

Criminal identity fraud can hit you in the face when you try to apply for a job. If your potential employer pulls a police report, they will see the black marks. The criminal records will show up even if it's fraudulent.

The mere fact that you have criminal records under your name can put you at risk of being called on by higher-ups. It's not pretty and it is downright shameful. Plus, you have to pay to clear your name.

If you are a victim, here is what you can do to protect yourself:

1. **Get in touch with an attorney.** They can give you legal counsel.
2. **Sign up for web monitoring services.** There's the dark web hovering behind everything. Sign up for a dark web monitoring service. They will alert you to any activity that happens in connection to your personal information on the dark web. This can help keep you in the know when your personal records are tampered with.
3. **Sign up for identity theft insurance.** Some dark web monitoring may come along with a \$1,000,000 identity theft insurance. That can go towards any fees you pay for legalities or for professionals to clean up from identity theft.

8. Protect Yourself from Fraud with your Medical Records

Where else will identity theft reach, you're thinking.

But identity theft may reach your medical insurance's pockets.

Medical identity theft is what happens when thieves use your personal information to receive medical insurance. They may actually stage a medical occurrence under your name just to be able to receive medical insurance.

The greatest damage this may have is to your medical records. There may be false medical incidents and information in your medical files. So number one, if you are a victim of identity theft or suspect fraud, please alert your doctors to it. They should know to check in with you regarding all details about your medical history before they make any medical decision.

What may also occur due to medical identity theft are credit collections. When a medical bill is not paid, the company can report it to the credit bureaus. The credit bureaus then place the unpaid bill on your credit report as a medical collection.

Medical collections are a delinquency on your credit report and your credit score will be affected negatively. Your credit score may drop if a new medical collection gets reported. Whatever medical tragedy the thief comes up with may evolve into a medical collection.

If you come across fraudulent medical collections on your credit report, report it as fraud and have the accounts removed. You have every right to dispute fraudulent accounts with the medical companies.

Check out this page to find out exactly how to get in touch with medical providers. Make sure to notify them of the fraud and ask them to remove the collections from your report.

9. Protect Yourself from Fraud with Your Investment Accounts

Lastly, your investment accounts. I'm sure you don't want anyone hacking into your investment accounts to deplete them of funds.

There are no laws in regards to protecting your investment accounts. So technically, you are on your own to deal with the catastrophe.

However, there are investment brokerages who do offer protection in case of identity theft.

The only step you can take to protect your investment accounts from identity theft is to sign up with a brokerage that has such protections in place.

As a matter of fact, I strongly recommend you only keep your investments with a company that offers protection against identity theft. These are some options. Check them out to see which one works for you:

Conclusion

We explored some ways identity thieves can hack into your personal and financial life.

It is no fun, whichever scheme they use, whatever account they break into. The least you can try to do is take the steps we encouraged in this post so that you can be as protected as possible from future identity theft. May you never fall prey.

The post Steps to Take to Protect Yourself if you are a Victim of Identity Theft appeared first on Due.

<https://www.entrepreneur.com/finance/steps-to-take-to-protect-yourself-if-you-are-a-victim-of/459139>