

12 Steps Toward Preventing Identity Theft

While there is no foolproof preventive, there are common sense approaches which will protect you under most conditions.

STEP

1

Guard your Social Security number

It's the prime target, for it leads to your credit report and your bank accounts. Do not print it on your checks. If you use it to apply for a loan, credit card, rental or anything requiring a credit report, ask that it be obliterated from the record and the forms returned to you once the transaction is completed. The lender really only needs your name and credit score.

STEP

2

Monitor your credit report *

You can arrange to be alerted to activity in your financial records. Once notified, you can follow up. Free Credit Reports are becoming available.

STEP

3

Buy a shredder and use it

Always destroy papers containing personal information before throwing them out. (A cross-cut shredder is best.)

STEP

4

Watch what you put in your trash

Items containing personal information, such as bank statements, credit card statements & receipts, etc., should not be thrown in the trash. Thieves may search trash for just this kind of information.

STEP

5

Remove your name from marketing lists

The three major credit bureaus maintain marketing lists which may contain your information. It is advisable to request that your name be deleted from these lists and from the Direct Marketing Association's mail and telephone preference service.

STEP

6

Keep duplicate records

Copy the contents of your wallet (both sides of each item) so that you have all your account numbers and other data in the event of loss or theft of a wallet or purse. Keep them in a safe and secure place such as a safety deposit box.

STEP

7

Know to whom you are speaking

On the phone, never release personal information unless you have initiated the call and trust the business with which you are dealing.

STEP

8

Be aware of your surroundings...

when using ATM cards, making credit card purchases and utilizing pin numbers and passwords.

STEP

9

Monitor...

credit card activity, bank statements and other financial accounts to ensure that all balances and receipts match. Review all statements when you get them. Close unnecessary department store or bank-issued credit cards.

STEP

10

Mail payments from a safe location

Mail boxes at private homes generally are not very secure. Do not place outgoing mail in your home mail boxes. Consider using a locked mail box to receive all mail.

STEP

11

If you use a computer...

install firewall and virus protection software. Be aware that it is possible that the personal information you send over the internet could be viewed by others. Make sure the site is secured.

STEP

12

Destroy...

computers, hard drives, floppy disks, compact discs and any other electronic recording device which may contain personal information prior to disposing of it.

*** Equifax • 800-685-1111 • www.equifax.com
Experian • 888-397-3742 • www.experian.com
TransUnion • 800-916-8800 • www.transunion.com**

Remember...it will be your responsibility to correct credit card errors and restore your identity.



If You are a Victim of Identity Theft...



NOTIFY! NOTIFY! NOTIFY!

Credit Bureaus

Immediately call the fraud unit of the three reporting companies. Ask to have your account flagged and have a "Fraud Alert/Victim Impact" statement placed on your credit file, asking creditors to call you before granting credit.

Obtain the names and phone numbers of the businesses where fraudulent accounts have been opened.

Review your credit report with them; request a copy.

Creditors

Contact your creditors and those who provided credit fraudulently, by phone and in writing to inform them of the problem. Ask for replacement cards; close old or fraudulent accounts, obtain new account numbers and pin numbers.

Law Enforcement

Contact your local Police Department, file a report and obtain a case number. Most credit card companies and financial institutions will require that you file a police report.

Post Office

Notify the US Postal Inspector:

(A) if you think someone has fraudulently changed your address; (B) if your mail has been stolen

Notify the local Postmaster for that address and instruct them to forward all mail addressed to you to the correct address.

Federal Trade Commission

(FTC)

The FTC is the clearing house for complaints by victims of identity theft. The FTC helps victims by providing information to help resolve financial and other problems that could result from identity theft. The forms and advice for reporting identity theft are available from the Federal Trade Commission — you may call 1-877-438-4338 or go to their web site:

WWW.CONSUMER.GOV/IDTHEFT.

The Fair Credit Billing Act limits the liability due to fraud to \$50 per card if the creditor is notified within 60 days of the first billing containing Fraud. In response to growing concerns about identity theft Congress passed the Fair and Accurate Credit Transaction Act (F.A.C.T.). The law requires companies to cooperate with consumers who believe that someone is fraudulently using their identity. It requires retailers to record only the last 5 digits of your credit card on a receipt. The law also says that all consumers who request a credit report are entitled to a free copy each year from all three credit bureaus. It calls for a one-stop streamlined system for reporting, instead of having to notify all three Credit bureaus.

With the crime of identity theft continuing to grow at epidemic proportions along with everyday activities such as check writing, charging gas or mailing a letter as possible invitations to an identity thief, our focus needs to shift to looking at how we do these things...for patterns or practices that can lead to our identities being stolen. F.A.C.T. is helpful—however, prevention is still your best defense.