

YOU THINK YOUR IDENTITY HAS BEEN STOLEN – WHAT TO DO

Fraud Prevention | Published: May 27, 2015

Even though you think you're keeping your personal information safe, there is still a chance that your identity could be stolen.

Last year, more than 13 million Americans are believed to have experienced identity theft. Of those, 332,000 reported it to the Federal Trade Commission.

What are the first signs your identity might have been stolen? And what can you do to minimize the damage before the thieves steal from your bank accounts, run up bills on your credit card, use your health insurance coverage or open new accounts in your name?



How you'll know when your identity has been stolen

Here are signs that someone may have stolen your identity, according to the Federal Trade Commission:

- You're notified of a data breach by a company where you do business.
- You see charges on your credit card that you didn't make.
- There are suspicious withdrawals from your bank account.
- You stop receiving your bills or other mail.
- You find unfamiliar accounts on your credit report.
- Merchants refuse your checks.
- Debt collectors call you about debts that aren't yours.
- Your health plan rejects your coverage because you're over your limit.
- Your health provider says you have an illness you don't have.
- The IRS notifies you that two tax returns have been filed in your name.

What to do when you realize you've been victimized

What is the first thing you should do? If you act quickly, you should be able to stop the identity thief from doing more damage.

First, place an initial fraud alert at one of the three national credit reporting companies – Experian, Equifax or TransUnion. The company your report it to will tell the other two. The fraud alert is free. It will help to prevent the identity thief from opening new accounts in your name.

Next, request your credit report and check it carefully.

Create an identity theft record by contacting government agencies such as the Federal Trade Commission or your police department to report the fraudulent activity.

Contact your bank, credit card companies and other institutions that you have financial dealings with, inform them of the theft and check your account statements for unusual activity.

If there are any companies you do not recognize on your credit statements, provide them with a copy of your police report or notarized Federal Trade Commission affidavit. To file a complaint with the FTC, call (877)-FTC-HELP or (877)-382-4357.

The Fair Credit Billing Act limits liability to \$50 when a consumer's card is used fraudulently.

Losses from your bank account through a debit card can be higher if the theft isn't reported immediately. The FTC has found that most identity theft victims do not ultimately experience any financial loss, although about 15 percent do. Most losses are less than \$100, but about 2 percent lose more than \$1,000, the FTC has found.

Medical identity theft is often more costly. A study by the Medical Identity Theft Alliance found that 65 percent of victims had a financial loss, with the average loss \$13,500. Some victims paid the healthcare provider for services received by the identity thief, repaid the insurer or engaged legal counsel.

Identity theft doesn't go away immediately – Follow-up

Once your identity has been stolen, it may take many calls and letters to resolve the situation. The loss of time involved can be considerably more costly than the financial loss.

It's important to create a system to track your progress, according to the Federal Trade Commission.

Log all telephone calls, recording the date, names and numbers of everyone you contact. Write down everything discussed.

Send letters by certified mail, keeping copies of the letter and return receipts.

File all documents, making copies when needed, and make a list of any deadlines that are requested by companies you are dealing with. Continue to review your credit report periodically to check for any new fraudulent activity.

The loss in time to correct a credit card problem averaged about three hours, according to an FTC survey of victims, while correcting a more complicated problem – such as an identity thief opening a bank account in the victim's name – took 30 hours or more. Victims of medical identity theft spend an average of 200 hours trying to resolve the issue, in part because of HIPAA privacy laws involved.

While half of the respondents to the FTC survey were able to resolve the identity theft problem in one day, for 7 percent, it took more than a year.

Some insurance companies offer identity theft insurance for expense reimbursement and assistance in the recovery process.