



IDENTITY THEFT: STEPS TO TAKE IF YOU ARE A VICTIM

If you suspect misuse of your personal information to commit fraud, take action immediately. Keep a record of all conversations and correspondence when you take the following suggested steps:

1) Contact all of your financial service companies (anywhere you have a financial account) immediately, as well as any insurer or agency you have purchased identity theft protection from (if applicable) so that the following can be done: access to your accounts can be protected; stop payments placed on missing checks; personal identification numbers (PINs) and online banking passwords changed; and a new account opened, if appropriate. Be sure to indicate to the bank or card issuer all of the accounts and/or cards potentially impacted including ATM cards, check (debit) cards and credit cards. Customer service or fraud prevention telephone numbers can generally be found on your monthly statements. Contact the major check verification companies to request they use their databases to notify participating retailers not to accept these stolen checks. In addition, ask your bank to notify the check verification service with which it does business. Three of the check verification companies that accept reports of check fraud directly from consumers are: Telecheck (800) 710-9898, International Check Services (800) 631-9656 and Equifax (800) 437-5120.

2.) File a police report with your local police department. Obtain a police report number with the date, time, police department, location, and police officer taking the report. The police report may initiate an investigation into the loss with the goal of identifying, arresting, and prosecuting the offender and possibly recovering your lost items. The police report will be helpful when clarifying to creditors that you are a victim of identity theft.

3.) Contact the three major credit bureaus and request a copy of your credit report. Review your reports to make sure additional fraudulent accounts have not been opened in your name or unauthorized changes made to your existing accounts. Check the section of your report that lists "inquiries." Request the "inquiries" be removed from your report from the companies that opened the fraudulent accounts. In a few months, order new copies of your reports to verify your corrections and changes to make sure no new fraudulent activity has occurred. Request a "fraud alert" for your file and a victim's statement asking creditors to call you before opening new accounts or changing your existing ones, which can help prevent an identity thief from opening additional accounts in your name. You can also place a freeze on your account. Here are the major credit bureaus and their phone numbers: Trans Union (800) 680-7289, Experian (888) 397-3742 and Equifax (800) 525-6285. Your

may also contact the FTC's ID Theft Consumer Response Center toll-free at (877) IDTHEFT.

4.) Be alert to sudden changes in anticipated mailings. Make sure no one has request an unauthorized address change, title change, PIN change, or ordered new cards or checks to be sent to another address. If a thief has stolen your mail to get credit cards, bank and credit card statements, pre-screened credit offers or tax information, or if an identity thief has falsified change-of-address forms, that's a crime. Contact your local post office and police.

5.) Maintain a written chronology of what happened, what was lost, and the steps you took to report the incident to the various agencies, banks, and firms impacted. Be certain to record the date, time, contact telephone numbers, person you spoke with, any relevant report or reference numbers, and instructions.