



Pennytree Advisers, LLC

Dan Candura, CFP®
 346 Washington St #65
 Braintree, MA 02184
 (781) 626-0888
 dan@pennytree.com
 www.pennytree.com



Recovering from Identity Theft



You've read about it, but you never thought it would happen to you. But suddenly your bank account is empty, your credit card bills are through the roof, and you're getting late notices for accounts you don't own. Your identity has been stolen. What now?

Time is money

To minimize your losses, act fast. Contact, in this order:

- Your credit card companies
- Your bank
- The three major credit bureaus
- Local, state, or federal law enforcement authorities

Your credit card companies

Credit card companies are getting better at detecting fraud; in many cases, if they spot activity outside the mainstream of your normal card usage, they'll call you to confirm that you made the charges. But the responsibility to notify them of lost or stolen cards is still yours.

If you do so in a reasonable time (within 30 days after you discover the loss), you won't be responsible for more than \$50 per card in fraudulent charges. Ask that the accounts be closed at your request, and open new accounts with password protection.

If an identity thief opens new accounts in your name, you'll need to prove it wasn't you who opened them. Ask the creditors for copies of application forms or other transaction records to verify that the signature on them isn't yours.

Follow up your initial creditor contacts with letters indicating the date you reported the loss or theft. Watch your subsequent monthly statements from the creditor; if any fraudulent charges appear, contest them in writing.

Organize your fight against crime

- *Be prepared with the information you'll need to give*
- *Keep a log of your conversations (dates, names of the people you speak with, and a summary of what's discussed)*
- *Follow up in writing*
- *Keep copies of your correspondence*
- *Keep the originals of supporting documents; send copies*
- *Keep old files even after the case is closed, just in case*

Your bank

If your debit (ATM) card is lost or stolen, you won't be held responsible for any unauthorized withdrawals if you report the loss before it's used. Otherwise, the extent of your liability depends on how quickly you report the loss:

- If you report the loss within two business days after you notice the card is missing, you'll be held liable for up to \$50 of unauthorized withdrawals. (If the card doubles as a credit card, you may not be protected by this limit.)
- If you fail to report the loss within two days after you notice the card is missing, you can be held responsible for up to \$500 in unauthorized withdrawals.
- If you fail to report an unauthorized transfer or withdrawal that's posted on your bank statement within 60 days after the statement is mailed to you, you risk unlimited loss.

If your checkbook is lost or stolen, stop payment on any outstanding checks, then close the account and open a new one. Dispute any fraudulent checks accepted by merchants in order to prevent collection activity against you. And notify the check-guarantee bureaus:

- Check Rite (800) 766-2748
- ChexSystems (800) 328-5121
- CrossCheck (800) 552-1900
- Equifax-Telecredit (800) 437-5120
- NPC (800) 526-5380
- SCAN (800) 262-7771
- Tele-Check (800) 366-2425

The three major credit bureaus

If your credit cards have been lost or stolen, call the fraud number of any one of the three national credit reporting agencies:

1. Equifax (888) 766-0008
2. Experian (888) 397-3742
3. TransUnion (800) 680-7289

You only need to contact one of the three; the one you call is required to contact the other two.

Next, place a fraud alert on your credit report. If your credit cards have been lost or stolen, and you think you may be victimized by identity theft, you may place an initial fraud alert on your report. If you become a victim of identity theft (an existing account is used fraudulently or the thief opens new credit in your name), you may place an extended fraud alert on your credit report once you file a report with a law enforcement agency.

Once a fraud alert has been placed on your credit report, any user of your report is required to verify your identity before extending any existing credit or issuing new credit in your name. For extended fraud alerts, this verification process must include contacting you personally by telephone at a number you provide for that purpose.

If you live in one of the handful of states that allow you to "freeze" your credit report, do so. Once you do, no one--creditors, insurers, and even potential employers--will be allowed access to your credit report unless you "thaw" it for them.

If your state allows you to freeze your credit report, you must contact all three major credit reporting agencies. In some cases, victims of identity theft are not charged a fee to freeze and/or thaw their credit reports, but the laws vary from state to state. Contact the office of the attorney general in your state for more information.

If you discover fraudulent transactions on your credit reports, contest them through the credit bureaus. Do so in writing, and provide a copy of the identity theft report you file. You should

Fraud alerts:

- *An initial fraud alert entitles you to one free credit report from each credit bureau, and remains on your credit report for 90 days*
- *An extended fraud alert entitles you to two free credit reports within 12 months from each credit bureau, and remains on your credit report for 7 years*

also contest the fraudulent transaction in the same fashion with the merchant, bank, or creditor who reported the information to the credit bureau. Both the credit bureaus and those who provide information to them are responsible for correcting fraudulent information on your credit report, and for taking pains to assure that it doesn't resurface there.

Law enforcement agencies

While the police may not catch the person who stole your identity, you should file a report about the theft with a federal, state, or local law enforcement agency. Once you've filed the report, get a copy of it; you'll need it in order to file an extended fraud alert with the credit bureaus. You may also need to provide it to banks or creditors before they'll forgive any unauthorized transactions.



When you file the report, give the law enforcement officer as much information about the crime as possible: the date and location of the loss or theft, information about any existing accounts that have been compromised, and/or information about any new credit accounts that have been opened fraudulently. Write down the name and contact information of the investigator who took your report, and give it to creditors, banks, or credit bureaus that may need to verify your case.

If the theft of your identity involved any mail tampering (such as stealing credit card offers or statements from your mailbox, or filing a fraudulent change of address form), notify the U.S. Postal Inspection Service. If your driver's license has been used to pass bad checks or perpetrate other forms of fraud, contact your state's Department of Motor Vehicles. If you lose your passport, contact the U.S. Department of State. Finally, if your Social Security card is lost or stolen, notify the Social Security Administration.

Follow through

Once resolved, most instances of identity theft stay resolved. But stay alert: monitor your credit reports regularly, check your monthly statements for any unauthorized activity, and be on the lookout for other signs (such as missing mail and debt collection activity) that someone is pretending to be you.

Disclosure Information -- Important -- Please Review

This information is not intended to be tax or legal advice. It is provided for your education only by Pennytree Advisers, LLC. Individual circumstances may vary.

