Dealing with Identify Theft

Fixing the damage done by identity thieves can be relatively simple or it could take months. Here's how to recover from two common forms of identity theft.

Unauthorized Charges or Checks

If you notice unauthorized charges on existing accounts, you're (sort of) in luck. This type of identity theft is relatively easy to repair, provided you act quickly.

As soon as you notice unauthorized charges on an existing account, contact your financial institution and explain your concerns. It's very important that you inform your financial institution quickly since your liabilities *increase* with time. For example, if you discover debit card fraud and report it within two business days, your liability is capped at $50. After two days, your liability could be as high as $500. After 60 days, you could be responsible for all fraudulent charges. Needless to say, if you even suspect that you have been a victim, contact the financial institution.

When you report credit or debit card fraud, your financial institution will cancel your existing card and issue an new one with a different account number. They will also ask that you identify the fraudulent charges and sign a legal statement (also called an affidavit) attesting that you did not make the identified charges. Finally, you may be issued provisional credit of the charges during their investigation. The process generally takes only a month or two, and your part is likely done after signing the affidavit.

For fraudulent checks, your financial institution will close your existing account, stop payment on any related checks, and provide a new checking account. You will then identify forged checks and follow a process similar to the debit / credit card situation outlined above. You will also need your bank to report the fraud to ChexSystems, a reporting agency similar to credit reporting agencies.

If you have automatic payments tied to an account that is closed (phone, gym, or insurance, for example), be sure to update the account information with the merchant as soon as possible. Otherwise, you could be charged late fees or experience service interruptions. It's your responsibility to update automatic payment accounts.

In most cases, unauthorized credit card charges can be cleared up quickly. If you were the victim of debt

New Accounts Established in Your Name

Compared with unauthorized charges, dealing with new accounts established in your name can be a much more lengthy and complicated process. Even identifying this type of identity theft is more difficult - you may not know that you have been a victim unless you regularly check your credit reports or get a collection letter for an account you never opened.

Below are the steps you should take to recover from this type of theft. Steps one through three should be done as soon as you notice a problem.

Step 1: Notify the Credit Bureaus

Experian, TransUnion, and EquiFax are the nation's major credit reporting agencies, and they are likely to maintain a file on your credit history. Contacting the major credit reporting bureaus is very important - they can place "fraud alerts" in your file (making it more difficult for criminals to establish new accounts) and they can work with you to remove fraudulent accounts.

An typical fraud alert stays in your file for at least 90 days. An extended alert stays in your file for seven years. To place either of these alerts, a credit reporting agency will require you to provide appropriate proof of your identity, including your Social Security number. If you ask for an extended alert, you will have to provide an identity theft report (see Step 2). For more detailed information about identity theft reports, visit www.consumer.gov.

Next, you can consider placing an optional security freeze on your credit reports. This step ensures that no one can access your credit report without your permission, but it can also lead to inconveniences when there's a legitimate reason for someone to access your report. Make sure you understand the pros and cons *before* requesting a security freeze.

After placing fraud alerts in your file, ask that the fraudulent accounts be removed from your report. In order to remove the inaccurate information, the credit bureau may need documentation from law enforcement and the Federal Trade Commission (see Step 2).

Note that the credit reporting agencies may try to sell you services related to protecting your credit report. These services are not required in order to fix identity theft.

Step 2: Contact Law Enforcement and Government Agencies

Report the identity theft to your local police department and possibly to the police departments of other areas in which the fraudulent activity may have taken place. Supply the police with as much information as possible and make sure all fraudulent accounts are listed on the police identity theft report. You will need a copy of their report for creditors of the stolen accounts. Make sure to keep the contact information of your investigator – you may need it later.

Identity theft reports may be made by local, state or federal agencies. If for some reason you are unable to get an identity theft report from your local police or sheriff's department, there are other options listed at www.ftc.gov/bcp/edu/microsites/idtheft/consumers/defend.html.

After you receive your identity theft report, report the crime to the Federal Trade Commission. While the Federal Trade Commission does not investigate identity theft crime, they do share information among investigators nationwide that may ultimately help you. The web address for this form is www.ftccomplaintassistant.gov. You will also want to complete the FTC's identity theft affidavit at www.ftc.gov/bcp/edu/resources/forms/affidavit.pdf. Many creditors and debt collectors accept this form, and you are likely to need it later.

If an identity theft scheme involved the mail, notify your local postal inspector. If your Social Security number has been used, notify the Social Security Administration. In some cases, new Social Security numbers are issued.

Step 3: Close Fraudulent Accounts

Contact the security or fraud department of each company where accounts have been tampered with or opened fraudulently. Follow up in writing, including copies of supporting documents such as your identity theft report and FTC affidavit. It's important to notify credit card companies and banks in writing. Send your letters by certified mail, return receipt requested, so you can document what the company received and when. Keep a file of your correspondence and enclosures. The FTC provides a form letter that you can modify to your personal situation at http://www.ftc.gov/bcp/edu/microsites/idtheft/downloads/Request-for-Fraudulent-Transaction.doc.

Step 4: Deal with Debt Collectors

Calls from debt collectors are a common occurrence in cases of identity theft. If a debt collector contacts you, tell the collector that you have been a victim of identity theft and are not responsible for the debt. Then ask for the contact information of the collector and the company, as well as for contact information for the creditor - including amount owed and account numbers. You will also need to supply them with a copy of your FTC fraud affidavit and/or identity theft report.

Ask the collection agency to forward copies of any documents related to your case and to notify the creditor that you are an identity theft victim (they are required to perform these tasks under federal law).

As with all other written correspondence related to your identity theft case, be sure to use certified mail with a return receipt.

Step 5: Continue to Monitor Credit Reports

Even if you remove all fraudulent information from your credit reports and close unauthorized accounts, you still need to monitor your credit reports. If the identity thief is not caught, he or she could try to use your information again - months or years in the future.

When you open new accounts, use new Personal Identification Numbers (PINs) and passwords. Avoid using easily available information like your mother's maiden name, your birth date, the last four digits of your Social Security number, your phone number, or a series of consecutive numbers.

In addition to the types of identity theft mentioned here, there are others types that may affect you: brokerage account fraud, Social Security number misuse, passport falsification, student loan fraud, driver's license fraud, and medical identity theft to name a few.

While these other types of identity theft are less common, you should still be aware that they do exist and may affect you.

Additional Resources

The resources listed here may be helpful depending on your situation.

We highly recommend visiting the FTC website for comprehensive descriptions of your rights under federal law.

Credit Bureaus

Experian
P.O. Box 2104
Allen, TX 75013-2104
Report Line: (888) 397-3742
Fraud Line: (888) 397-3742
www.experian.com

TransUnion
P.O. Box 1000
Chester, PA 19022
Report Line: (800) 888-4213
Fraud Line: (800) 680-7289
www.transunion.com

Equifax
P.O. Box 740241
Atlanta, GA 30374
Report Line: (800) 685-1111
Fraud Line: (888) 766-0008
www.equifax.com

Free Credit Reports

Annual Credit Report Request Service
P.O. Box 105281
Atlanta, GA 30348-5281
877-322-8228
www.annualcreditreport.com

Government Agencies

U.S. Federal Trade Commission (FTC)
FTC Consumer Response Center
877-ID-THEFT
www.ftc.gov

U.S. Postal Service
877-876-2455
postalinspectors.uspis.gov

U.S. Social Security Administration
Report Line: 800-269-0271
Benefit Estimate Line: 800-772-
www.ssa.gov

Check-Related Issues

If you cannot open a checking account because of identity theft, contact:

Chexsystems
7805 Hudson Road
Suite 100
Woodbury, MN 55125
www.consumerdebit.com
800-428-9623