Dealing with Identity Theft

What is Identity Theft?

In an increasingly inter-connected world, the possibility of having private personal and financial information deliberately stolen or accidentally exposed to unauthorized eyes is widely seen as a growing risk. The term "Identity Theft," (ID Theft) is used to describe a situation where such personal information – normally private – is somehow made "public" and then used for an illicit or criminal purpose.

Identity Theft Often Results in Fraud

Common types of ID Theft fraud include:

- **Financial fraud:** Existing account fraud involves essentially "taking over" an existing checking or savings account, draining funds from the account, or running up excess charges on a credit card. New account fraud involves creating new checking, savings, or credit card accounts; the victim is often not aware that these accounts have been opened.
- **Tax identity fraud:** An identity thief can use a stolen Social Security Number (SSN) to file an income tax return, receive a refund, and then disappear before the legitimate owner of the SSN can file his or her own return. A stolen SSN can also be used in schemes involving welfare fraud, unemployment fraud, or Social Security benefit fraud.
- **Child identity fraud:** Some individuals will use a child's identity to obtain credit. With this type of fraud, it may be years before the cime is discovered.
- **Medical identity fraud:** Medical ID fraud is used to illegally obtain medical treatment or supplies.

What to Do If You're a Victim of Identity Theft

Although the specific details will vary from case to case, if you're a victim of ID Theft you'll generally go through these steps:

1. Contact the fraud department of the institution involved. You will need to explain that your identity has been stolen. The affected accounts will need to be closed or frozen so that no new withdrawals or charges may be made. It's also a good idea to change passwords, PINs, and log-in names.

2. Contact one of the three major credit bureaus[1] and set up a "fraud alert." A fraud alert is a warning on your credit file that credit issuers should take extra precautions before granting credit to someone claiming to be you.

    - **Equifax:** https://www.equifax.com/
    - **Experian:** https://www.Experian.com/
    - **TransUnion:** https://www.Transunion.com/

    Once you have set up a fraud alert with one of these three credit reporting bureaus, the other two bureaus will be notified. A fraud alert lasts 90 days, is free to set up, and can be renewed as many times as you feel is necessary. Each time a consumer sets up or renews a fraud alert, the consumer is entitled to a free copy of his or her credit report from each credit reporting bureau. If an individual is confirmed to be a victim of ID Theft, he or she can set up an extended fraud alert, for up to seven years.

3. Review your credit report to identify accounts or transactions that you don't recognize. This will help later when making any reports to authorities.
4. Consider setting up a credit "freeze." A credit freeze effectively closes (except for existing accounts and certain government agencies) your credit report until you lift or remove the freeze. There may be a fee involved to set up a credit freeze and you'll need to contact each of the credit reporting bureaus separately.
5. Consider reporting the identity theft to appropriate authorities:

    - **Federal Trade Commission (FTC):** The FTC maintains a website dedicated to dealing with ID Theft at https://www.identitytheft.gov/. The website allows you to document what happened and helps to develop a step-by-step plan to recover from the theft. Having reported and documented the theft can help later with getting fraudulent information removed or blocked from your credit report. It can also help in dealing with creditors and debt collectors from reporting and attempting to collect debts you didn't incur.
    - **Your local police:** Report the ID theft to your local police or law enforcement. A police report can provide additional support when disputing fraudulent charges.

[1] You may also wish to contact a fourth, smaller credit bureau, Innovis, at https://www.innovis.com/.

6. Begin repairing the damage. This may involve a number of steps:

    - Closing new accounts fraudulently opened in your name and opening new, valid accounts to replace them.
    - Removing fraudulent charges from your accounts.
    - Correcting your credit report.
    - Defending yourself against debt collectors seeking to recover debts you didn't create.

Preventing Identity Theft

As the foregoing list makes clear, clearing your name after someone steals your identity and uses it fraudulently can involve enormous time and effort. There are things that can be done to prevent – or minimize - the damage from ID Theft. Some basic steps might include:

- **Check your credit report regularly:** Consumers are entitled to one free credit report each year from each of the major credit reporting bureaus.
- **Check your accounts regularly:** Internet access allows an account owner to check an account more frequently than the usual monthly statement. Limiting the number of checking or credit card accounts can facilitate this process.
- **Be safe on the internet:** Always use security software with a firewall and anti-virus protection. Create passwords that are complex and difficult to break. Learn to recognize and avoid "phishing" (pronounced "fishing") e-mails asking you to click on a link and provide personal data. When shopping on the internet, check out companies you buy from to be sure they are legitimate.
- **Protect portable devices:** Portable devices such as cell phones and laptop computers need to be protected. At a minimum, any device with a screen needs a strong password to access the device.
- **Telephone calls and texts:** Be aware that threatening calls and texts can come from identity thieves posing as legitimate organizations such as your bank, credit card, or even the IRS.

Other Resources

There are a number of internet resources available to help individuals learn about and deal with ID Theft:

- **Federal Trade Commission:** https://www.identitytheft.gov/
- **Consumer Financial Protection Bureau:** https://www.consumer.gov/articles/1015-avoiding-identity-theft
- **Internal Revenue Service (IRS):** https://www.irs.gov/identity-theft-fraud-scams/identity-protection
- **Privacy Rights Clearinghouse:** https://www.privacyrights.org/
- **ID Theft Resource Center:** https://www.idtheftcenter.org/