

Warning Signs

There are several warning signs that can tip you off to a problem.
Be sure to look out for:

- ✓ Phones calls or suspicious mail that arrives addressed to the child, such as pre-approved credit cards or debt collection material.
- ✓ A credit report that already exists in the child's name.
- ✓ A financial account that already exists in the child's name.
- ✓ Strange notices or requests from the Internal Revenue Service (IRS), such as:
 - Notices that indicate your child has failed to pay income taxes when no income was earned.
 - Requests to confirm your child's employment when your child is unemployed.
 - Notices that indicate your child's information is listed on a tax return other than your own.

My Child's Identity Was Stolen, What Now?

If your child's identity was stolen, there are steps you can take to remedy the situation:

- ➔ Obtain a credit report with your child's personal information by contacting the three credit agencies:
 - Equifax: 1-800-525-6285
 - Experian: 1-888-397-3742
 - Trans Union: 1-800-680-7289 or
childidtheft@transunion.com
- ➔ If any fraudulent activity is detected, immediately file an identity theft complaint with your local police precinct and report findings with the three credit agencies.
- ➔ Place a freeze on the child's credit record to prevent further damage.
- ➔ File an online complaint with the New York Department of State's Division of Consumer Protection at www.dos.ny.gov or call our Consumer Assistance Hotline at 1-800-697-1220.

Be alert to phishing, SMiShing, and other identity theft scams by regularly checking the NYS DOS Division of Consumer Protection's website at www.dos.ny.gov.

Safeguarding Your Child's Identity

What are
the warning
signs?

Can I prevent
this from
happening?

Stolen?
What now?

A Tool to Aid Parents & Caregivers

provided by:

**New York State
Department of State**

**Division of
Consumer Protection**

www.dos.ny.gov 1-800-697-1220

A product of the New York Department of State
Division of Consumer Protection's Identity Theft and Mitigation Program

Anyone can fall prey to identity theft, even children. Child identity theft presents its own unique set of challenges. Thefts continue to rise as minors and young adults are targeted for their unused social security numbers. Being aware of child identity theft and knowing the steps to take to prevent it is the best line of defense.

Child identity theft occurs when a minor's personal information is used to create a false identity, which usually includes the commission of fraud. The false identity is then used to obtain credit cards, open new utility accounts, or make large purchases, such as a car or home, in the name of the child victim. Children's identities are especially attractive to identity thieves because often the theft of the child's identity remains undetected for years. For many child victims, the realization that their identities have been stolen does not occur until the first time they attempt to open a bank account, apply for a job, seek credit, or rent an apartment.

This brochure serves as a tool to aid parents and guardians in preventing child identity theft, identifying signs that a child may be a victim, and responding and mitigating any damage inflicted upon a child victim's identity.

Remember to talk to your child about the importance of Internet safety and securing their personal information. Review all websites on which your child participates and approve the submission of any personal identifying information.

If asked for a social security number, inquire *why is it needed?* Is there another way to identify my child? How will my child's information be protected? Only reveal your child's Social Security number if you have no other option.

Preventing Child Identity Theft

Take the following steps to safeguard your child from identity theft:

- ✓ Keep birth certificates, social security cards and other personal information safely locked away.
- ✓ Only provide social security numbers when absolutely necessary.
- ✓ Shred papers with personal information before discarding.
- ✓ Protect electronic files containing personal information with passwords and delete files when no longer needed.
- ✓ Remove all previously-stored personal and financial information from any electronic devices that are being sold, recycled or disposed.
- ✓ Before you allow your children to use the Internet, teach them about what information is private and should not be shared online.
- ✓ Set privacy settings on social media websites to a secure level to protect your children.
- ✓ Use passwords that are at least eight characters long and contain a combination of letters, numbers, and symbols. Change passwords frequently and never share them.
- ✓ When using a shared computer, log off websites and the terminal after each use. Update computer anti-virus software and ensure firewall protection is turned on.
- ✓ Never send personal information through unsecured wireless connections in public places.
- ✓ Check the level of security for each website used by looking for the padlock icon on the right side of the address bar and a URL that begins with "https."

Don't provide personal identifying information to after-school activities and sports clubs upon registration!