



Protecting your child's identity

Minors make ideal targets for identity thieves because they have a clean credit history and the crime could go undetected until the minor becomes an adult and applies for credit of their own. With that in mind, an identity thief could misuse the child's information for nearly two decades before it is detected.

When children are born, parents apply for a Social Security number, which is all that's required to open most credit accounts. In the wrong hands, a child's Social Security number can be used to apply for government benefits, open bank and credit card accounts, apply for a loan or utility service, or rent a place to live. The damage to a child's credit could be expensive and time-consuming to repair and could hinder the child's ability to secure student loans, purchase a vehicle, or apply for a job.

Warning signs

Several signs can tip you off to the fact that someone is misusing your child's personal information and committing fraud. For example, you or your child might:

-  Be turned down for government benefits because the benefits are being paid to another account using your child's Social Security number.
-  Get a notice from the IRS saying that the child did not pay income taxes, or that the child's Social Security number was used on another tax return.
-  Get collection calls or bills for products or services you did not receive.

If you think your child's information is at risk:

-  **Check your child's credit report.** The credit reporting agencies do not knowingly maintain credit files on children. A check of your child's credit should turn up nothing until the age of 18 unless they are a victim of identity theft or a secondary user on a credit card where a parent may authorize a child to make charges on their card.

Request a manual search of the child's file with each credit reporting agency. The companies will check for files relating to the child's name and Social Security number, and files related only to the Social Security number. The credit reporting companies may require copies of:

- The child's birth certificate listing parents
- The child's Social Security card
- The parent or guardian's government-issued identification card, like a driver's license, or copies of documents proving the adult is the child's legal guardian

- Parent/guardian proof of address, like a utility bill, credit card or insurance statement

Contact the credit bureaus below for more information on how to request manual searches.

Equifax (CSC)

(800) 525-6285

Experian

(888) 397-3742

TransUnion

childidtheft@transunion.com

 **Get a police report.** If your child's identity has been compromised, file a police report. Be sure to keep copies on file. You will need the report to prove your child is a victim.

 **Check for an earnings statement from the Social Security Administration.** Unless your child is old enough to work, there should be no earnings associated with his social security number. You can get an earnings statement by requesting it online at www.ssa.gov. You can also call the Social Security Administration at (800) 772-1213 or visit your local office.

Prevention = Protection

You can take steps to protect your child's identity from misuse:

 **Place a security freeze on your child's credit record** to prevent anyone from opening a new credit account in their name. Contact the credit bureaus below for more information on security freezes for minors.

Equifax https://help.equifax.com/app/answers/detail/a_id/779

Experian <https://www.experian.com/consumer/help/states/wi.html>

TransUnion <http://www.transunion.com/personal-credit/credit-disputes/ProtectedConsumers.page>

 **Find a safe location** for all paper and electronic records that show your child's personal information.

 **Do not share your child's Social Security number** unless you know and trust the other party. Ask why it is necessary and how it will be protected. Ask if you can use a different identifier, or use only the last four digits of your child's Social Security number.

 **Shred** all documents that show your child's personal information before throwing them away.

 **Warn your children** not to give out personal information unless it is vitally important and exchanged with a reliable source. Explain to them that they should not provide such information, especially online.

 **Be leery of credit offers to your children.** Opt-out of pre-approved credit card offers on behalf of your child by going online at www.optoutprescreen.com or by calling 1-888-966-2255.

 **Be aware of events that put information at risk.** For example, there is an adult in your household who might want to use a child's identity to start over; you lose a wallet, purse or paperwork that has your child's Social Security information; there is a break-in at your home; school, doctor's office or a business notifies you that your child's information was affected by a security breach.

 **Understand website privacy policies.** The Children's Online Privacy Protection Act (COPPA) requires websites to obtain parental consent before collecting, using or disclosing information about a child who is under the age of 13. Websites and applications should spell out your rights as a parent, to review and delete your child's profile.

Limiting the risks of child identity theft

Laws safeguard your child and your family's personal information. For example, the federal Family Education Rights and Privacy Act (FERPA), enforced by the U.S. Department of Education, protects the privacy of

student records. It also gives parents of school-age children the right to opt-out of sharing contact or other directory information with third parties, including other families.

If you are a parent with a child in school:

-  Find out who has access to your child's personal information. Verify that the records are kept in a secure location.
-  Pay attention to forms from the school. Forms that ask for personal information may come home with your child, or you may get them through the mail or email. Look for terms like "personally identifiable information," "directory information," and "opt-out." Find out how your child's information will be used, whether it will be shared and with whom.
-  Read the notices from your child's school. The school will send home an annual notice that explains your rights under FERPA. Including your right to:
 - Inspect and review your child's education records.
 - Approve the disclosure of personal information in your child's records.
 - Ask to correct errors in the records.
-  Ask your child's school about its directory information policy. Student directory information can include your child's name, address, birth date, telephone number, email address, and photo. If you want to opt-out of the release of directory information to third parties, it is best to put your request in writing and keep a copy for your files. If you do not opt-out, directory information may be available to the people in your child's class and school, and to the general public.
-  Ask for a copy of the school's policy on surveys. The Protection of Pupil Rights Amendment gives you the right to see surveys and instructional materials before they are distributed to students.
-  Consider other programs that take place at the school. Your child may participate in programs, like sports and music activities that are not formally sponsored by the school. These programs may have websites where children are named and pictured. Read the privacy policies of these organizations to find out if – and how – your child's information will be used and shared.
-  Take action if your child's school experiences a data breach. The school or the school district may notify you of a data breach. If not, and you believe your child's information has been compromised, contact the school to learn more. Talk with teachers, staff, or administrators about the incident and their practices. Keep a written record of your conversations. Write a letter to the appropriate administrator, and to the school board, if necessary.

For more information or to file a complaint, visit our website or contact the Office of Privacy Protection.

**Bureau of Consumer Protection
Office of Privacy Protection
2811 Agriculture Drive
PO Box 8911
Madison WI 53708-8911**

E-MAIL: DATCPWisconsinPrivacy@wi.gov

WEBSITE: privacy.wi.gov

(800) 422-7128

(608) 224-5163

FAX: (608) 224-4677

TTY: (608) 224-5058