CHILD IDENTITY THEFT
WHAT YOU NEED TO KNOW

prevention tips to share with your friends and family

What is Child Identity Theft?

Child identity theft happens when someone uses a minor's personal information to commit fraud. A thief may steal and use a child's information to get a job, government benefits, medical care, utilities, car loans, or a mortgage. Avoiding, discovering, and undoing the damage resulting from the theft of a child's identity can be a challenge.

Adults can monitor their own credit reports every few months to see if someone misused their information, and order a fraud alert or freeze on their credit files to help stop more misuse. But most parents and guardians don't expect their child to have a credit file, and as a result, rarely request a child's credit report, let alone review it for accuracy. A thief who steals a child's information may use it for many years before the crime is discovered. The victim may learn about the theft years later, when applying for a loan, apartment, or job.

Warning Signs of Child Identity Theft

Identity theft can be committed by a family member, a neighbor, or by someone you never met who gets access to your child's information. Several signs can tip you off to a problem:

- You get calls from collection agencies, bills from credit card companies or medical providers, or offers for credit cards or bank account checks in your child's name.
- Your child, or your family, is denied government benefits because benefits are being paid to another account that is using your child's Social Security number.
- The Social Security Administration, Internal Revenue Service (IRS), or other government agency asks you to confirm that your child is employed, even though your child has never had a job.
- After you file a tax return listing your dependent child's name and Social Security number, the IRS tells you the same information is listed on another tax return.
- Your child gets a notice from the IRS saying he or she failed to pay taxes on income, even though your child has no income.

South Carolina Department of Consumer Affairs
2221 Devine St. STE 200 · PO Box 5757 · Columbia, SC 29250
800-922-1594 · www.consumer.sc.gov

ACTION STEPS

How To Protect Your Child's Information

Parents do a lot to protect their children from physical harm, but protecting their personal information is important, too. Here's how:

- Keep all documents that show a child's personal information locked up. This is includes a child's date of birth, Social Security number, and birth certificate. **Don't carry your child's Social Security card in your purse or wallet.**
- If someone asks for your child's Social Security number, ask why they want it, how they'll safeguard it, how long they'll keep it, and how they'll dispose of it. If you're not satisfied with the answers, don't share the number and ask to use another identifier. Remember to ask these questions even when you register your child for school, also making sure to read the notices schools are required to send explaining your rights under the Family Educational Rights and Privacy Act (FERPA).
- Consider using the protected consumer freeze. The freeze allows the parent, guardian or representative of the protected consumer to create a credit file in that person's name and place a freeze on it, helping to deter identity theft.
- Before you share personal information on the internet, make sure you have a secure connection. A secure website has a lock icon in the address bar and a URL that begins with "https."
- Use a computer with updated antivirus and firewall protection. Don't send personal or financial information – your child's or your own, for that matter – through unsecured Wi-Fi.

THE PROTECTED CONSUMER FREEZE

A protected consumer is someone under the age of 16 or an incapacitated adult. Remember to place your request with EACH of the three credit reporting agencies listed below. The credit reporting agencies must place the freeze within 15 days of receiving your request. This protective measure is **FREE**.

Detailed instructions on placing the protected consumer freeze can be found at www.consumer.sc.gov. Click REPORT IDENTITY THEFT, then click *Taking Advantage of the Protected Consumer Freeze.* Directions can also be mailed by request, simply call 800-922-1594.

How To Teach Your Child To Protect Their Information

Talk with your child regularly about the privacy settings on social media sites and what information and photos to share on them. For example, it's not a great idea to show photos with school or team uniforms, list birth dates or specific locations, or show background settings that are easy to identify. Why? Someone can use the information posted on a social media profile to guess account passwords.

Your computer can hold lots of information, and it's important that it stays secure. Talk to your child about best practices for computer security, including:

- Using "strong" passwords – those with at least eight characters, as well as numbers and symbols.
- Keeping passwords private and using anti-virus software that updates automatically.
- Knowing the risks of sharing files through peer-to-peer software, which may give someone access to more information on your computer than you want to share.
- Being alert to phishing scams, where criminals send an email, text, or pop-up message that looks like it's from a real organization. A phishing message asks the recipient to click on a link or call a phone number, and to share personal information for a prize or some other benefit. **Bottomline: delete these messages without opening or responding.**