

ID Theft – A Growing Risk
Part 2 of a 2-Part Series: What Can You Do?
© Johanna Fox Turner, CPA, CFP, RLP

In last month's article, we discovered that most people are totally unaware of a disturbing new threat to our children's privacy. Because identity thieves remain invisible until caught, they can have up to 18 years to use a youngster's information until the child reaches maturity and drops into the cesspool of ID theft. This month, we have suggestions to help you reduce the risk to children.

Social Security numbers ("SSN") are stolen in a variety of ways. You may lose your wallet with your card inside. You could fail to protect your number, such as sending it by email. Someone you have entrusted with your number may carelessly leave it for others to see. Most significantly, online thieves have begun targeting organizations that store vast amounts of children's Social Security numbers, such as health care providers and schools. But those agencies often fail to properly safeguard the information or to promptly disclose data breaches when they occur. Even worse: they may wait months to report they've been hacked as they try to do "damage control". This gives the thieves a head start on their unsuspecting targets.

Checking your child's credit report

Children should not have a credit report before age 18 because kids can't legally contract for credit. An existing report is typically either a mistake or the result of fraud. An exception to that rule is if a child is an authorized user on a parent's credit card. However, repeated calls to check your child's credit can result in a credit file being opened, which you want to avoid – so what should you do?

When a child turns 16, you should check with all three credit reporting agencies for existence of a report. This allows two years to resolve any problems that may turn up. CreditCards.com has an excellent printable list detailing how to get your child's credit report. In the meantime, be on the alert for signs of child ID theft, which include getting a preapproved credit card offer in the mail or a debt collection call for your child.

Foster children are particularly vulnerable to ID theft because their personal information is transferred frequently and many adults have access to their personal records.

Be proactive

There is no easy way to prevent the theft of a child's identity but here are some tips:

1. Familiarize yourself with the online world. "You can't protect your kids' privacy online, and you can't protect your kids' finances online, unless you know how online works," said Alan Simpson, vice president of policy for Common Sense Media, a child advocacy group.
2. Always use virus-protection and filtering software. ID theft often occurs when thieves use a virus to download information.
3. Adopt a policy of not giving out a SSN unless you're convinced it is necessary. In fact, you may have noticed that entities now often request only the last four numbers, which is a good thing. However, it's hard to imagine why your church would need your child's number on a release form for camp. Ask for an explanation of the need, who will have access to it, and how the number will be disposed

of. Try to stay on top of who has access to your SSN. See [Social Security Online](#) for “Legal requirements to provide your SSN.”

4. Do not carry ANYBODY’S Social Security card in your wallet except for situations when it is required, such as the first day of a new job.
5. If your bank, credit union or other financial service provider uses your Social Security number as a personal identification number (PIN) or as the identifier for banking by phone or the Internet, write a letter of complaint.
6. Because Social Security numbers may be predicted based upon your birthday, age, and place of birth, avoid sharing this information on the Internet.
7. Talk to teens about limiting what they share on social media. “[Staying Private in Public](#)”, a guide from the California Office of Privacy Protection, is an excellent guide for all ages.
8. Consider using an ID protection service -- some of which are free -- for all members of the family.
9. Obviously, you should never use your SSN in public, especially on checks and ID cards, and never email it to anyone.
10. And finally, don’t forget about good old-fashioned shredding!

If you know where to look, there is a wealth of free information on the internet. You can find an excellent [Guide to Online Security](#) at the Consumer Reports website. In addition, the nonprofit [Identity Theft Resource Center](#) has a wealth of information and can help guide you in the event of attack. The [Identity Theft Assistance Center](#) (ITAC) is a national advocate for identity theft victims and leading voice on identity policy, providing free services to its customers. [AllClearID](#) offers both free and monthly billing monitoring services.

Anne Wallace, executive director of ITAC, suggests you think of Social Security numbers as cash to help focus on who you are giving them to and for what purpose. This is very serious business: a clean SSN may allow an illegal alien to gain employment, which can be life-changing for a person desperate enough to steal one.

The consequences of having your identity stolen are many. Victims are denied credit, including college loans, can have motor vehicle records linked to criminals, cannot get an apartment, cannot open a utility account or buy a cell phone, can have medical records muddied with incorrect information, and more. Identity thieves can cause years of turmoil for a young adult, turning what should be a happy time into a financial nightmare. Do what you can now to avoid that “pound of cure” later!

[Email me](#) your questions or comments.

Fee  Only

907 Paris Road, Ste B
Mayfield, KY 42066
phone: 270.247.0555
fax: 270.247.2080
toll free: 800.991.2721
www.milestonesfp.com