consumer action

Education and advocacy since 1971

# Child ID Theft


Adults aren't the only ones who can have their identity stolen. Tens of millions of American children had their Social Security numbers, date of birth and health care ID numbers stolen in the early-2015 data breach at health insurance giant Anthem Inc. This exposes these kids to the real risk of identity theft. "Criminals will use those stolen Social Security numbers to open accounts, get medical treatment, commit tax fraud, you name it," predicted Adam Levin, chairman and founder of IDentityTheft 911, in an NBCNews.com article.

**Child ID theft**: According to the Federal Trade Commission (FTC), child ID 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, a car loan or a mortgage. Avoiding, discovering and undoing the damage resulting from the theft can be a challenge. A thief who steals a child's information may use it for years before the crime is discovered. How? Well, most parents or guardians are not checking their child's credit file—they may not even realize they have one. The child victim may learn of ID theft only years later, when applying for credit, a job, an apartment or insurance.

According to the FTC, there are a few signs that can tip you off to the theft: (1) A child or a family is denied government benefits because benefits are being paid to another account that is using the child's Social Security number; (2) You are getting calls from collection agencies, bills from credit card companies or medical providers, or offers for credit cards or bank accounts in your child's name, even if your child has never applied for or used these services; (3) After you file a tax return listing your child's name and Social Security number, you get a notice from the IRS saying that the same information is listed on another return; and (4) Your child gets a notice from the IRS stating that he or she failed to pay taxes on income, even though your child has no income.

**Who typically steals a child's identity?** According to Equifax credit reporting agency, there are two categories of people who are stealing and using children's identifying information:

- **Unknown perpetrator:** Thieves that have either stolen or purchased the Social Security number and sometimes other identifying information of a child.
- **Family members:** A reality of child identity theft is the fact that parents or family members of a child have been found to use the child's identifying information, often in a time of desperation.

If you think your child's information is at risk—specifically, you see warning signs, or you may have lost your child's Social Security card, had a break-in, or your child's information was compromised in a data breach at school or in a doctor/dentist office—you may want to check whether your child has a credit report. According to the FTC, you should contact each of the three national credit reporting agencies in writing to request a manual search of your child's file. Each agency will check for files relating to the child's name and/or Social Security

number**. There is a sample letter in the MoneyWi$e ID theft lesson plan** (www.consumer-action.org/downloads/english/ID_Theft_Lesson_2014.pdf) that can be used to request the check. The credit reporting agencies may require copies of the child's birth certificate listing the parents; the child's Social Security card; and the parent or guardian's government-issued ID proving the adult requesting the search is the child's parent or legal guardian.

**Protect your child's personal information at school**: According to the FTC, the federal Family Educational Rights and Privacy Act, enforced by the U.S. Department of Education, protects the privacy of student records. It also gives parents of school-age kids the right to opt out of sharing information. A copy of the FTC's fact sheet "Protecting Your Child's Personal Information at School" can be downloaded at www.consumer.ftc.gov/blog/protecting-your-childs-personal-information-school.

**Recovering from child identity theft**: The three credit reporting agencies have specific child identity theft webpages with information, instructions, and forms to check and report a false credit report.

**Protecting foster kids' credit**: Children and youth in foster care are particularly vulnerable to ID theft because their personal information is often shared among caretakers, service providers and schools. The misuse of the child's identity may not be discovered until s/he exits the foster care system and applies for a cell phone, job, apartment or student loan. In 2011, Congress passed legislation to help youth in foster care better protect their credit. Now, when a foster child turns 16, child welfare agencies are required to get the youth's annual credit report. In cases of ID theft, the agency must help the youth clear up their credit. The FTC and Child Focus, Inc. created a guide entitled "Youth and Credit: Protecting the Credit of Youth in Foster Care" to provide anyone working with these young people with the tools to help if their identity has been stolen, and to teach teens about credit, why it is important to their future financial stability, and how bad credit can derail their goals. A copy can be downloaded at www.aecf.org/resources/youth-and-credit/.

**Resources:**

Child Identity Theft Education Kit (Equifax): www.equifax.com/specs/child-identity-protection-kit/child-kit.pdf
Child Identity Theft (TransUnion): www.transunion.com/childidentitytheft
"Safeguarding Your Child's Future" (FTC): www.consumer.ftc.gov/articles/pdf-0010-child-identity-theft.pdf
Child Identity Theft (FTC): www.consumer.ftc.gov/articles/0040-child-identity-theft

Free ChildScan Report (AllClear ID): www.allclearid.com/plans/child/

1. If you become aware of any fraudulent transaction, immediately report it to the institution, and follow up by formally disputing the transaction in writing.
2. Be suspicious of any email or phone call that you might receive about the breach that requests personal information.

**What if the breach involves your Social Security number?** If the breach involves exposure of your Social Security number, a thief could use the information to open new accounts in your name. Although research firm Javelin Strategy & Research revealed in its report released in March 2015 that new account fraud hit a record low in 2014, it continues to be one of the most damaging types of fraud. Privacy Rights Clearinghouse recommends that if you receive notice that your Social Security number was compromised in a breach you should take the following steps:

1. Notify credit reporting agencies and immediately place a fraud alert on your credit report.
2. Order your credit reports and examine them carefully for signs of fraud.
3. Consider a security freeze. It provides the greatest protection from ID theft.
4. Be suspicious of any email or phone call that you may receive about the breach that requests personal information.

**What if the breach involves your driver's license number or another government-issued ID?** If the breach notification indicates that your driver's license or another government-issued ID was compromised, you should contact the agency that issued the ID and ask what they recommend. As noted by Privacy Rights Clearinghouse, you may be instructed to cancel the ID and obtain a replacement, or the agency may "flag" your file to prevent an imposter from getting a license or other ID in your name.

**Know your rights**: According to the National Conference of State Legislatures (NCSL), 47 states, the District of Columbia, Guam, Puerto Rico and the Virgin Islands have enacted legislation requiring private and/or government entities to notify individuals of security breaches of information involving personally identifiable information. You can find a list of state laws at NCSL's website (www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx).

In addition to state law, federal law may require notice for certain types of data breaches. For example, the federal Gramm-Leach-Bliley Act requires financial institutions to adopt procedures to safeguard customer data and notify customers when there has been unauthorized access to it. The HITECH Act requires the Department of Health and Human Services (HHS) to issue rules defining how and when consumers are to be notified of a breach of protected health information. You can check to see if your medical provider has reported a data breach at the HHS website (www.hhs.gov/orc/privacy.hipa.adminstration.breachnotificationrule/).

**Resources:**

Chronology of Data Breaches (Privacy Rights Clearinghouse): www.privacyrights.org/data-breach

CFPB Issues Consumer Advisory on Industry's Data Breach (CFPB): www.consumerfinance.gov/newsroom/cfpb-issues-consumer-advisory-on-industrys-data-breach/

$16 Billion Stolen from 12.7 Million Identity Fraud Victims in 2014 (Javelin Strategy): www.javelinstrategy.com/news/1556/92/16-Billion-Stolen-from-12-7-Million-Identity-Fraud-Victims-in-2014-According-to-Javelin-Strategy-Research/

Data Breach Reports (ITRC): www.idtheftcenter.org/images/breach/DataBreachReports_2014.pdf

May 2014 Intersections Consumer Notification Guide (Intersections Inc.): www.intersections.com/library/Consumer_Notification_Guide_May%202014_Final.pdf

Federal Trade Commission ID theft hotline: 877-438-4338

Annual free credit reports: www.annualcreditreport.com

*Consumer Action empowers low- and moderate-income and limited-English-speaking consumers nationwide to financially prosper through education and advocacy. Visit us online at www.consumer-action.org.*