

CONSUMER NEWS SAN DIEGO CITY ATTORNEY'S OFFICE

Children's Identity Theft

May 2012

Identity theft occurs when someone uses the personal identifying information of another person to obtain money or services. According to the California Office of Privacy Protection, about 8.1 million adults in the United States were victims of identity theft in 2010.

However, identity theft targets victims of all ages, not just adults. In some cases, identity thieves target children because they can use the stolen information for many years without being detected. Parents often do not learn of the theft until the child reaches adulthood.

This newsletter will give tips on how to safeguard a child's identity. It will also outline steps that should be taken if your child's personal information has been compromised.

PREVENTIVE MEASURES:

One of the best ways to prevent identity theft is to limit who has access to your child's personal information (Social Security number, medical record number, bank account information, etc.).

- Safely store your child's personal documents in a secure location.
- Limit who has access to your child's personal information on a needto-know basis.
- Ask why someone needs your child's personal information, how they will store it, and how they will dispose of it.
- Remember, even trusted friends and family members have been known to take on a child's identity. A child's personal information can be abused by someone who is looking for a way to

- start over with a new financial identity.
- Instruct your child to ask you for permission before giving away any personal information.

TIPS:

Even seemingly innocuous sources can get your child's personal information into the wrong hands. School forms often require parents to provide the child's personal information.

- Find out from the school:
 - Who has access to your child's personal information?
 - How is the information stored?
 - How long will the information be kept?
- Carefully read the materials sent home with your child that request personal

information. The forms may be sent by programs that take place on campus but are not sponsored by the school. In such cases, also be familiar with the privacy policy of the program.

➤ The Family Educational Rights Privacy Act (FERPA) gives parents the option to opt out of the disclosure of the child's personal information to third parties.

SIGNS YOUR CHILD'S PERSONAL INFORMATION MAY HAVE BEEN COMPROMISED:

The Federal Trade Commission has identified several signs that indicate your child's identity may have been compromised:

- > Calls from collection agencies;
- > Offers for credit cards or bank accounts in your child's name;
- > A notice from the Internal Revenue Service (IRS) that your child's Social Security number is being claimed as a dependent on another tax return;
- > Denial of government benefits because your child's Social Security number is getting benefits through another account: or
- ➤ Notice from the IRS that your child has failed to pay income taxes.

TIPS:

If you believe your child's personal information has been compromised you may want to check your child's credit report.

The three major credit reporting agencies normally do not keep files on minors. Call them to see if they have a file linked to your child's name and Social Security number.

- ➤ If you are told that they do not have a file linked to your child's name and Social Security number, follow up in writing to each of the credit bureaus to confirm that information. Ask that they send the confirmation in writing as well.
- > If you are told that there is a file in your child's name or Social Security number, get a credit report to inspect your child's credit history. Also call each of the bureaus to initiate a fraud alert on your child's file and to begin the process of clearing your child's credit history.

The following resources will give you more detailed instructions on how to contact credit reporting agencies to check your child's credit history, how to set up a fraud alert or credit freeze, and how to clean up a child's credit history:

http://www.privacy.ca.gov/cons umers/security child.pdf

http://www.ftc.gov/bcp/edu/pub s/consumer/idtheft/idt08.pdf

ENFORCEMENT:

Identity theft can be reported to the Federal Trade Commission by phone at 1(877)-438-4338 or online at

www.ftc.gov/complaint

You should also report identity theft to your local police department.

San Diego **City Attorney's Office Consumer and Environmental Protection Unit** (619) 533-5600

This newsletter was written by City Attorney Intern Stacey Kim.

Sources: CA Penal Code § 530.5 et. seq.; FTC Consumer Alert, "Protecting your Child's Personal Information at School"; FTC Publication May 2012, "Safeguarding Your Child's Future"; California Office of Privacy Protection Website; California Office of Privacy Protection Publication, "What to do if your Child's Social Security Number has been Compromised."

The information provided in this newsletter is intended to convey general information and is not intended to be relied upon as legal advice.

To report violations of consumer protection laws, call the City Attorney's Hotline at (619) 533-5600.