PROTECT YOUR CHILDREN—AND YOURSELF—AGAINST IDENTITY THEFT

Billions of people were affected by data breaches and cyber attacks in 2019, according to CNBC. Identity Theft Resource Center listed some of 2019's biggest breaches as Quest Diagnostics (11.9 million records), Houzz (48.9 million records), Capital One (100 million records), Dubsmash (161.5 million records) and Zynga (218 million records). While you are probably aware of your own risk of identity theft and maybe have taken some precautions to guard your own personal and financial data, have you protected your minor children? Experian reports more than 1.3 million children each year are victims of identity theft. Worse, identity theft on a child can go on for years undiscovered. Most victims don't find out about it until they are young adults and find their credit rating compromised or are rejected for student loans, jobs or from renting a place to live.

What are the warning signs that your child's credit history may have been compromised?

- Your child is denied a bank account or a driver's license;
- Credit card/loan offers come to your house addressed to your child;
- Collection calls or bills addressed to your child; or
- A notice from the IRS that your child owes income taxes or was claimed as a dependent on another return.
- What you can do before and after a possible data breach?
- Check your child's credit history. There are three recognized companies that can assist with this process:
    1. Equifax (www.equifax.com/personal/education/identity-theft child-identity-theft/)
    2. Experian (www.experian.com/fraud/form-minor-child.html)
    3. TransUnion (www.transunion.com/credit-disputes/child-identity-theft-inquiry-form)

How can you repair the damage?

1. Act quickly.
2. File a police report as applicable.
3. Notify all financial institutions involved.
4. File your taxes as early as possible.
5. Create an identity theft file and keep copies of everything.
6. Change all passwords.
7. Obtain new credit cards and destroy the old ones.
8. Monitor unusual activity with your mail, Social Security account and health insurance.
9. Contact all three credit reporting companies (see above) and ask them to remove any files that have your child's Social Security number listed.
10. Place a fraud alert with the applicable entity on the credit report.
11. File a fraud report with the FTC online (identitytheft.gov) or call (877) 438-4338.

Use these steps for prevention and protection:

- Find a safe location for papers and electronic records;
- Use a crosscut or microcut shredder to shred documents with personal information;
- Don't share your child's SSN unless you know and trust the other party;
- Ask at your child's school or medical office how your child's information is collected, stored, used and thrown away;
- Be aware of events that may put information at risk, like a break-in at your child's school, doctor's office or in your home;
- Before your child turns 16, get a credit report. If there are errors due to fraud, you will have time to correct them before your child applies for a job, a loan for tuition or needs to rent an apartment;
- Teach your children to keep personal information private when they are online. Social networking sites can be a goldmine for identity theft thieves. Do not put full birth dates or personal information such as where they go to school, their pets' names or their favorite anything if it's used in conjunction with a password;
- Check all bank accounts regularly;
- Check credit card statements regularly;
- Freeze your credit with credit reporting companies to prevent anyone from opening a credit account in your name. However, that also includes you, so you will need to unfreeze your account if you are applying for any kind of loan or credit;
- Secure your computer. Don't stay logged in and use passwords and personal identification numbers (PINs) if possible;
- Do not open email attachments from unknown sources;
- Secure personal data in your home. Don't leave wallets or anything else with ID cards or credit cards out in the open;
- Keep this information confidential:
    1. Social Security number;
    2. Credit/debit card numbers;
    3. Driver's license number;
    4. Bank account numbers;
    5. Birth dates;
    6. PIN numbers;
    7. Medical records; and
    8. A mother's maiden name (often used for verification).
- Shred critical documents;
- Do not give out vital information on the telephone;
- Before giving out your Social Security number ask why the business needs it, if there is an alternative ID number you can use or what will happen if you refuse to give it;
- Write "Photo ID Required" on the back of your credit cards; and
- Destroy unwanted credit card offers.

Any taxpayer who believes they are at risk of identity theft due to lost or stolen personal information should contact the IRS immediately so the agency can take action to secure his or her tax account. The taxpayer should contact the IRS Identity Protection Specialized Unit at (800) 908-4490. He or she will be asked to complete the IRS Identity Theft Affidavit, Form 14039, and follow the instructions on the back of the form based on their situation

The IRS has issued guidance for actual or potential identity theft, phone scam and phishing victims. Visit irs.gov/identity-theft-fraud-scams or check with your CPA for recommendations regarding identity theft protection services.