

PROTECTING YOUR KIDS FROM SYNTHETIC IDENTITY FRAUD



Fraud can affect many different types of populations with devastating effects. However, what is even more disheartening is that children are popular targets for certain types of fraud.

Synthetic identity fraud is the use of a combination of personally identifiable information to fabricate a person or entity in order to commit a dishonest act for personal or financial gain.

Fraudsters target the use of children's Social Security numbers (SSNs) in synthetic identity creation, as they are typically not being actively used until the child is in his or her late teens. What makes your child's information so valuable?

- The (typically) unused SSN can be paired with any name and birthdate to create a synthetic identity.
- The probability of discovery is usually extremely low, as parents typically don't monitor their children's identities or credit scores.

The impact of synthetic identity fraud on a child's future may be profound. It could prevent, or significantly damage, the child's future ability to obtain employment; acquire student loans; acquire services such as housing, phone service and utilities; or secure a general credit line or bank account.

Additionally, once fraud is discovered, the burden of proof will likely be on you to convince the credit bureaus and financial institutions that the SSN belongs to your child and not the synthetic identity. This is because the industry typically assumes the first person to establish credit under an SSN is the legitimate owner.

HOW CAN YOU PROACTIVELY REDUCE THE RISK OF YOUR CHILDREN BECOMING VICTIMS OF SYNTHETIC IDENTITY FRAUD?

- Keep your children's sensitive documents such as SSN cards, birth certificates and medical records in a safe and secure location.
- Avoid sharing too much information about your child, both online and in person. Fraudsters are always looking for general information about minors so they can expose and obtain their personal information.
- When your children are old enough, teach them about guarding their information, as well. This includes not sharing their private personal information with friends via social media or gaming groups.



PROTECTING YOUR KIDS FROM SYNTHETIC IDENTITY FRAUD



- Work with the credit bureaus to freeze your child's credit. When your child is born, the ability for them to use the SSN is defaulted to open or available. As your child is not likely to need the SSN until their late teens, a credit freeze can prevent fraudsters from using their SSN to create a synthetic identity and commit fraud using the identity. Visit these websites to begin the process of requesting a credit freeze or security freeze from each of the credit bureaus:

- [Equifax](#)
- [Experian](#)
- [TransUnion](#)

HOW DO YOU KNOW IF YOUR CHILD'S INFORMATION HAS BEEN COMPROMISED?

- Check with the credit bureaus to see if your child has a credit report in his or her name. This is a possible red flag that his or her SSN has been compromised.
- The Federal Trade Commission (FTC) offers a list of **warning signs** that someone has stolen your personal information.

WHAT SHOULD YOU DO IF YOU FIND THAT YOUR CHILD HAS ALREADY BEEN TARGETED?

The FTC also offers the following resources to help individuals whose personal information has been exposed or stolen in some way and then used by another.



DETECTING THE PROBLEM:

A **checklist of important personal information** and what to do for each type of information that is lost or exposed.



PROTECTING YOUR KIDS FROM SYNTHETIC IDENTITY FRAUD



REPORTING THE PROBLEM:

A [step-by-step guide](#) for reporting when someone is using your personal or financial information to make purchases, get benefits, file taxes or commit fraud.



MOVING FORWARD AND REBUILDING:

A [personal recovery plan](#) that walks you through each step of the recovery process and provides you with the ability to update and track progress of the personalized plan.

This website offers other resources - such as pre-filled forms, documents and letters - that can be sent to credit reporting agencies, businesses and debt collectors regarding the stolen information. For more information on resources offered by the FTC, visit: [IdentityTheft.gov](https://www.ftc.gov/identitytheft).

TAKE ACTION

Increasing your awareness of how your children may be affected by synthetic identity fraud is the first step in protecting them. Then, by being diligent in both monitoring their credit and safeguarding their personal information, you can help reduce the risk of your children being victims of this type of fraud.

The synthetic identity fraud mitigation toolkit was developed by the Federal Reserve to help educate the industry about synthetic identity fraud and outline potential ways to help detect and mitigate this fraud type. Insights for this toolkit were provided through interviews with industry experts, publicly available research, and team member expertise. This toolkit is not intended to result in any regulatory or reporting requirements, imply any liabilities for fraud loss, or confer any legal status, legal definitions, or legal rights or responsibilities. While use of this toolkit throughout the industry is encouraged, utilization of the toolkit is voluntary at the discretion of each individual entity. Absent written consent, this toolkit may not be used in a manner that suggests the Federal Reserve endorses a third-party product or service.

