Key Private Bank

Protecting family finances from child identity theft and fraud

Identity theft and fraud are not issues limited to adults—children are an often-overlooked vulnerability.

In fact, 2017 saw more than one million children become victims of identity fraud, totaling $2.6 billion in losses and $540 million in costs to families, according to Javelin Strategy & Research.[1]

The latest statistics from the U.S. Department of Justice (DOJ) show how complex and invasive identity theft can be—two-thirds of victims report a direct financial loss, and those who spend more than a few months resolving the issue are more likely to experience problems with work and personal relationships, as well as severe emotional distress.[2]

When it comes to children, identity theft can be even more complex. With little financial history to start, children can become long-term victims. Additionally, children are often victims of "familiar fraud": Identity theft committed by someone familiar to the family who likely has access to children's personal information.

Protecting children and family wealth from fraud requires an understanding of what comprises identity theft, how fraudsters do it, and what preventative measures parents can take.

What is identity theft?

The DOJ defines identity theft and identity fraud as all types of crimes in which someone wrongfully obtains and uses another person's personal data in some way that involves fraud or deception.

Families might see this when they get a bill for a credit card and there is a charge for a purchase in New York City at a time when they were home in Cleveland. Perhaps they'll receive calls from a collection agency for a loan in a young child's name that they never applied for.

The information that identity thieves typically target:

- Name, address, and birth date
- Social Security number
- Financial account numbers
- Personal identification number (PIN)
- Credentials for logging into online accounts, such as username, password, and answers to security questions

The Facts of Child Identity Theft:

2x

Fraudsters steal on average twice as much from children than adults.[1]

67%

of child identity fraud victims are seven years old or younger.[1]

60%

of child victims of identity fraud personally know the fraudster.[1]

How identity thieves steal information.

Personal information is all around all the time. The internet is easily searchable, mail is left in mailboxes, and retail data breaches are common.

Some methods identity thieves use to gain access to personal information:

- Spying in public, such as looking over your shoulder at an ATM, eavesdropping on personal conversations, watching you enter phone numbers, and listening to credit card numbers given over the phone
- Scanning cards given to them as servers
- Placing card scanners on public or unsecured, private ATMs
- Mining mail and paperwork that was thrown out, but not shredded or destroyed, such as pre-approved credit cards
- Email “spam” or “phishing”
- Large computer and storage data breaches

How to prevent and deal with child identity fraud.

Family wealth is always at risk, given how easily personal information can be stolen, but each family member can and should help to reduce this risk of loss. In addition to identity theft risk protection products—which work similarly to auto, life, and home insurance—parents should build personal habits they can pass down to their children and help protect them for the long-term.

Preventing child identity fraud:

1. **Train children to protect their identity,** particularly as they navigate the digital world. Show them how to spot scams and when to withhold information.
2. **Teach children precautionary lifestyle habits** to prevent identity thieves from accessing their personal information in public and at home, in addition to online.
   For example, they should avoid private ATMs and should never give out their Social Security number to anyone who calls them.
3. **Familiarize yourself and your family with potential scams,** such as email phishing attacks that children may not be able spot on their own or suspicious phone calls from the IRS—the IRS never calls citizens directly.
4. **Actively monitor and freeze family members’ personal credit reports.** Plan to freeze family members’ credit reports, regardless of their respective ages, until an action is taken that requires access to their file.
5. **Connect with your advisor to determine your family’s exposure** to cyber risks and to assess a potential need for cyber insurance.

Key Private Bank

Did You Know?

The Economic Growth, Regulatory Relief, and Consumer Protection Act, which became law in September of 2018, allows parents to freeze their children's credit files for free. Fraud alerts have also been extended to allow for longer monitoring periods.[3]

Recovering from child identity fraud:

1. **Immediately report identity theft attacks** to local police—many financial institutions require it as part of their investigation. Be sure to also contact the breached company and set up credit monitoring.
2. **Change your financial account settings**—both digital access and account recovery information—to ensure that any compromised information is updated. Remember to work with your advisor to safely record new settings.
3. **Take advantage of available financial resources and seek help** from your advisor. Remember, financial advisors should have your children's best interests and financial futures in mind, as well as your own.
4. **Check your children's credit reports and scores annually** and review them for signs of fraudulent activity.
5. **Consider contacting the Federal Trade Commission** and your state or local consumer protection agency to help resolve the issue.

For more information, please contact your Key Private Bank Advisor.

Key Private Bank

[1]2018 Child Identity Fraud Study, Javelin Strategy & Research.
[2]Victims of Identity Theft, Bureau of Justice Statistics.
[3]United States Congress Website. https://www.congress.gov/bill/115th-congress/senate-bill/2155.