CHILD IDENTITY THEFT REPORT 2012

Identity Thieves Target Young Children: What Parents Need to Know to Protect their Kids

By Jamie May, Chief Investigator, AllClear ID

AllClear ID
ALERT NETWORK

EXECUTIVE SUMMARY

Some say a child is a blank slate, something that has yet to be marked or written upon, pure, new and without a history. Often to parents, this means that a young child represents opportunity, options and the potential of a bright and limitless future. Though some may question this notion of a blank slate from a psychological or sociological standpoint, one thing is for certain: a child's identity *is* a blank slate. It is clean, unmarred, and untouched and so it *should* be. Unfortunately, with the high rate of child identity theft, more and more parents and their children are finding this not to be the case.

An identity thief sees your child's unused Social Security number as a free ride. This is why it is so important for parents to protect their children's valuable information before they're old enough to do so themselves. Imagine watching your child take a first step toward independence by trying to get a credit card, college loan, or lease an apartment, only to be rejected because of someone else's negative credit or even criminal or history.

Child identity theft does not *only* happen to other people; it can happen to any child. Last year's ground-breaking Child Identity Theft Report 2011 revealed some shocking statistics and started the conversation about this serious issue – an issue that many people did not even realize existed. Still, many parents do not realize how this theft happens and what they can do to prevent it. Worse yet, many parents are misinformed on how to find out if their child is a victim and what to do about it if he or she is.

Amazingly, child identity theft is much more prevalent than adult identity theft with children being targeted 35 times more often than adults. The data in this new report also reveals that the younger the child, the better as this give the thief more time to use the child's identity undetected. **In fact, the percentage of victims under the age of five doubled this year compared to last year's report.**

Child Identity Theft 2012 is not based on survey data. It is based on extensive database scans of actual accounts (credit, utilities, employment) opened by real companies using children's Social Security numbers. AllClear ID scanned 27,000 American children and found nearly 3,000 cases of child identity theft. This study provides a detailed analysis along with stories of real victims and the serious impact child identity theft has had on their families, financially and emotionally. This report will define child identity theft and explain how it can happen to any child. It will also highlight what parents need to know and do to protect their children, along with solutions for those who find themselves already victimized by this crime.

©2012 AllClearID. All rights reserved. No part of this publication may be used, reproduced, photocopied, transmitted or stored in any retrieval system of any nature, without the written permission of the copyright owner.

KEY POINTS INCLUDE

1. **The percentage of victims under the age of 5 more than doubled this year compared to last year – an increase of 105%.** Identity thieves seem to be targeting younger victims possibly because they can use their information undetected for a longer period of time.

2. **Child identity theft often goes undetected because children do not use their Social Security number for credit until they become an adult.** Adults use their identities regularly to apply for things like loans, credit cards, jobs, and home loans. Children, however, typically do not begin using their information until early adulthood. It is not uncommon for the theft of a child's identity to go undetected until she turns 18 and tries to use her information for the first time.

3. **Many parents and experts think checking their children's credit reports are all they need to do to determine if their children are identity theft victims; however, this is not an effective solution to uncover this problem.** This is because a credit report only checks the history of a Social Security number (SSN) as linked to a specific name and date of birth. Identity thieves often attach your child's Social Security number to a different name and date of birth. As a result, credit reports fail to detect 99% of child identity theft cases.[1]

4. **Identity theft can have a devastating impact on a child's life.** It can affect her ability to get a student loan, scholarship, internship/job, and credit card, among other things. The financial costs of identity theft are sometimes dismissed because it is usually the bank that ends up incurring the losses. However, once victimized, the child will likely be blocked from opportunities and experiences in early adulthood – a cost that is much harder to quantify.

Credit reports fail to detect 99% of child identity theft cases.

©2012 AllClearID. All rights reserved. No part of this publication may be used, reproduced, photocopied, transmitted or stored in any retrieval system of any nature, without the written permission of the copyright owner.

TABLE OF CONTENT

©2012 AllClearID. All rights reserved. No part of this publication may be used, reproduced, photocopied, transmitted or stored in any retrieval system of any nature, without the written permission of the copyright owner.

SUMMARY OF 2012 CHILD IDENTITY THEFT DATA

1. 2,875 or 10.7% of children had someone else using their Social Security numbers. This is an increase of .5% from the 10.2% rate reported in the 2011 report.

2. The rate of identity theft for children was 35 times higher than the rate for adults in the same population.

3. Criminals are targeting the youngest children. 15% of victims were five-years-old and younger, an increase of 105% over the 2011 findings and 26% of victims were six to ten-years-old, a 34% increase from the 2011 report. This stands in sharp contrast to the rates for children over eleven that remained flat or decreased.

4. Child identity thieves used their victims' Social Security numbers to open credit cards and secure auto loans, student loans, mortgages, and business lines of credit, among other things.

5. $ 1.5 million was the largest fraud committed. This was against a 19-year-old girl whose Social Security number had been used since she was nine-years-old.

6. One child had six suspects using her Social Security number. Overall, the number of suspects per child increased by 15% this year over the previous year's report.

15% of victims were five-years-old and younger, an increase of 105% over the 2011 findings

©2012 AllClearID. All rights reserved. No part of this publication may be used, reproduced, photocopied, transmitted or stored in any retrieval system of any nature, without the written permission of the copyright owner.

METHODOLOGY

Child Identity Theft 2012 contains no survey data. It is based on extensive database scans of actual accounts (credit, utilities, employment) opened by real companies using children's Social Security numbers. Scans on 26,989 children were performed between September 1st, 2010 and December 31st, 2011.

OVER
$1,000,000
IN FRAUD

REAL-LIFE VICTIM
Olivia 19-years-old, *Florida*

When Olivia, now 19, went off to college she and her mother thought it would be a good idea for her to get her first credit card to begin to build her credit and financial independence. Olivia applied for a card, but was denied and told that the Social Security number on her application did not belong to her. It turns out that an identity thief had been using her Social Security number since she was ***9-years-old. During this time he was able to open over 40 accounts*** *including credit cards, auto loans, three or four mortgages. and possibly even a business line of credit.* ***The total estimated fraud was over $1.5 million.***

Resolution:
AllClear ID is in the process of returning Olivia's information to its pre-fraud status and currently working with law enforcement to assist in the criminal investigation of the suspect involved.

The participants were enrolled in AllClear ID protection either after receiving notification that their personal information may have been compromised during a data breach or after enrolling in protection services on their own. The report only includes victims from data breaches when the incident showed no evidence of harm to the victims. The attack rate for adults affected by these same data breaches is very low at 0.3%, which is below the national average of 1% for the general population for new account fraud.[2]

The data from the Child Identity Theft Report 2012 seems to indicate that identity thieves recognize the value of an unused Social Security number and, as a result, are targeting children, especially young children. It highlights a serious threat and raises important questions that could provide some crucial insight and information if they were the subjects of scientific studies.

©2012 AllClearID. All rights reserved. No part of this publication may be used, reproduced, photocopied, transmitted or stored in any retrieval system of any nature, without the written permission of the copyright owner.

INTRODUCTION

Most parents try to do everything they can to ensure their children's health and safety. Very often, this starts even before their children are born when their mothers begin taking prenatal vitamins and preparing their homes for a new baby. Parents buy items like the latest infant car seats and baby monitors and diligently research and interview pediatricians, baby-sitters and day care centers and take infant and child First Aid classes. When their children become toddlers, preschoolers and older, parents teach them about the stranger dangers that exist in real life and online. Unfortunately the threat of identity theft is one that few parents know to protect against. This threat can be devastating to a child's financial and reputational health and can delay their transition towards independence in young adulthood.

Adult identity theft is a more commonly discussed crime. A great deal of information is available to consumers on how to prevent, detect, and resolve it, if they do end up a victim. However, children are more valuable targets and child identity theft is a crime many parents are not familiar with, much less aware of how to prevent or correct if it is already occurring.

As our data shows, when left undetected the losses can be staggering. In the case of one 19-year-old girl from Florida, the thief was able to accumulate an astonishing $1.5 Million in charges over an almost 10 year span. The report also indicates that thieves are targeting younger children. This shows that there is "more value and more time to use a fresh Social Security number. It allows thieves to apply a whole other level of creativity that you can't do with an adult who already has an established record in the commercial databases," explains Bo Holland, founder and CEO of AllClear ID.

Imagine, having a six, seven or eight year old child who owes more on a mortgage than you make in a year? Or one who has years of unpaid credit card or medical bills associated with his or her information? Unfortunately, these situations are a reality for 10.7 % of the children scanned in this report. "In many cases, these victims don't even know what 'credit' and 'debit' mean, and in some cases they are not even old enough to say those words out loud," said Mary Lou Leary, Acting Assistant Attorney General at the Office of Justice Programs at the July 2011 Stolen Futures Forum.[3] It is disturbing that identity thieves set out to steal identities of children long before these children have a chance to establish anything for themselves. Fortunately there are now steps parents can take to protect their children.

Imagine, having a six, seven or eight year old child who owes more on a mortgage than you make in a year?

©2012 AllClearID. All rights reserved. No part of this publication may be used, reproduced, photocopied, transmitted or stored in any retrieval system of any nature, without the written permission of the copyright owner.

WHAT THE DATA REVEALS

The data examined for Child Identity Theft 2012 includes the identity scans of 26,989 minors.

Minors who showed activity associated with their Social Security number ranged from infants to 18-year-olds:

- Cases involving identities of minors ages 5-years-old and younger: 426
- Cases involving identities of minors ages 6 to 10-years-old: 759
- Cases involving identities of minors ages 11 to 14-years-old: 843
- Cases involving identities of minors ages 15 to 18-years-old: 848

The largest increase from 2011 to 2012 was in the 5-years-old and younger category – which experienced 105% growth in the number of victims.

FIVE CREDIT CARD ACCOUNTS

TWO STUDENT LOANS

REAL-LIFE VICTIM

Bradley, 18-years-old, *California*

One identity thief was linked to Bradley's Social Security number. This thief had opened five credit cards with a cumulative high balance of ***$7,625*** *and two student loans with a cumulative high balance of* ***$11,595****. This identity theft began when Bradley was just 8-years-old.*

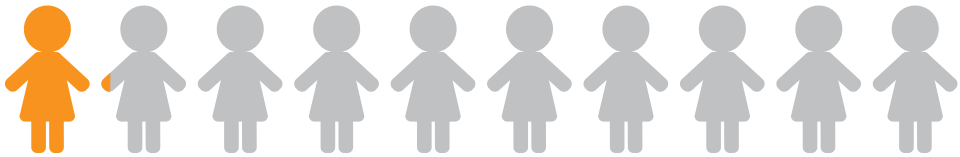
Resolution:
AllClear ID is continuing to work the case to ensure Bradley will not be held responsible or further impacted by this fraud.

SOME INTRIGUING DATA POINTS FROM THIS REPORT INCLUDE:

- Overall 15% increase in the average number of records per child from 2011 to 2012.
- The number of cases in which a child's Social Security number appeared in credit bureau records: 6,273 (Note: Within each case, there can be multiple records connected to a single child.)
- The number of cases in which a child's Social Security number appeared in utility service records: 2,352. This is an increase from last year's report when this number was 1,767.
- The number of cases in which a child's Social Security number appeared in records related to property assessments, deeds, mortgages and foreclosures: 1,459 This is an increase from last year's report when the number was 537.
- The number of cases in which a child's Social Security number appeared in driver's license records: 214
- The number of cases in which a child's Social Security number appeared in vehicle registration records: 345 This is an increase from last year's report when this number was 235.

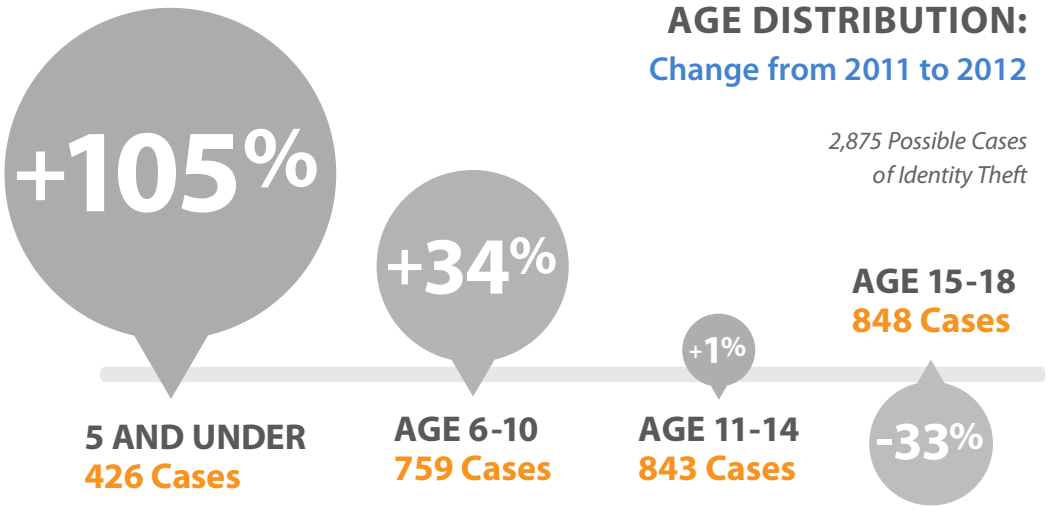
©2012 AllClearID. All rights reserved. No part of this publication may be used, reproduced, photocopied, transmitted or stored in any retrieval system of any nature, without the written permission of the copyright owner.

2012 CHILD IDENTITY THEFT RESEARCH RESULTS: GRAPHS & CHARTS

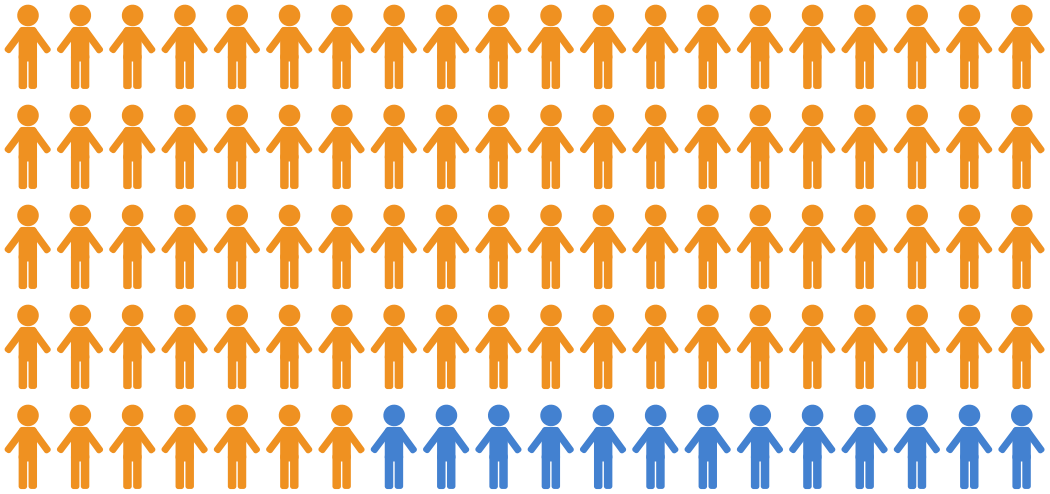


10.7% Percentage of child identities scanned revealed evidence of identity theft.

Total: *26,989 Minors Identities Scanned,* ***Time Period:*** *9/10 – 12/11*



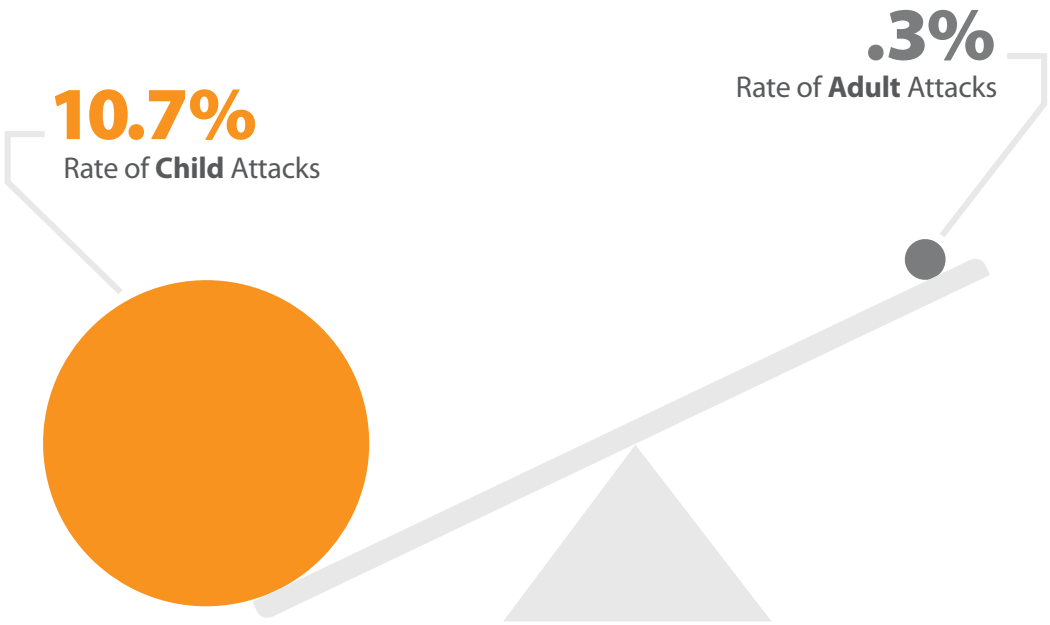
©2012 AllClearID. All rights reserved. No part of this publication may be used, reproduced, photocopied, transmitted or stored in any retrieval system of any nature, without the written permission of the copyright owner.



87%
Fraud

13%
File Contamination/ Mixed file**

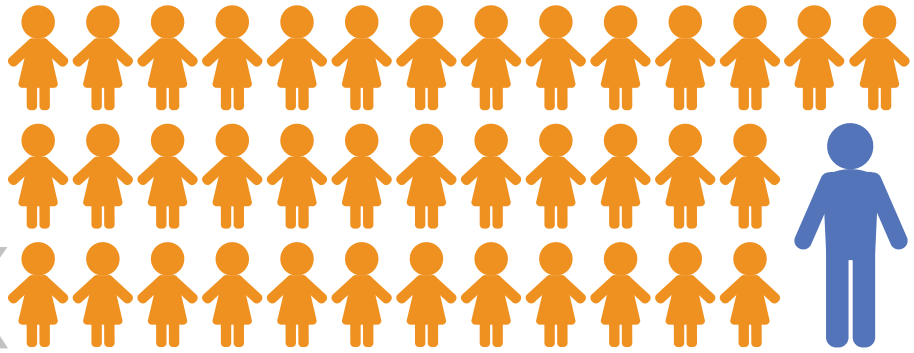
Note: *File Contamination/Mixed File indicates events caused by mistakes in reporting, not fraud. The impact to the child is the same as fraud in that the child is unable to use their Social Security number; it is assigned to someone else.*



©2012 AllClearID. All rights reserved. No part of this publication may be used, reproduced, photocopied, transmitted or stored in any retrieval system of any nature, without the written permission of the copyright owner.

Children are

35x



more likely to be victims than adults.

TYPES OF RECORDS INVOLVED IN CHILD IDENTITY THEFT CASES

59%
Credit Bureau
6273 Records

2% **Drivers License**
214 Records

3% **Vehicle Registration**
345 Records

14%
Property Assessments, Mortgages, Foreclosures, Deeds
1459 Records

22%
Utility
6273 Records

Total Cases: 2,875

Note: *Data includes cases in which child may be affected by more than one type of identity theft, resulting in a higher total of record types than children.*

©2012 AllClearID. All rights reserved. No part of this publication may be used, reproduced, photocopied, transmitted or stored in any retrieval system of any nature, without the written permission of the copyright owner.

The data also reveals that child identity theft is much more prevalent on a percentage basis than adult identity theft. 10.7% (2,875) of these 26,989 minors had their Social Security numbers linked to loans, utility accounts, property assessments and deeds, mortgages, foreclosures, driver's licenses, vehicle registration and other accounts. This is 35 times higher than the 0.3 % identity theft rate for adults in the same time period.

THIS IDENTITY CRISIS

CHILD IDENTITY THEFT DEFINED

Child identity theft is when someone fraudulently uses personal information belonging to a child under the age of 18, as per the Federal Trade Commission. Identity thieves typically steal and utilize this information for financial reasons such as to get a job, credit card or car loan, lease an apartment or even buy a house. They also use it to avoid having negative information associated with their real identity, like when being processed for a crime.

OVER
$170,592
IN FRAUD

REAL-LIFE VICTIM

Hannah 16 years of identity theft

Hannah's scan revealed multiple suspects had been using her Social Security number since she was 2-years-old. They had established two mortgages, and an installment account. Over the years, ***$170,592 worth of credit had accumulated*** *and by the time her identity theft was detected there was still* ***$82,037 of debt****. When she applied for a bank card to use in college, she was rejected because the bank's credit check found an estimated $16,000 in debt linked to her Social Security number with their institution alone.*

Resolution:
AllClear ID removed the fraud and closed the case.

HOW CHILD IDENTITY THEFT HAPPENS

For many people, how this crime is actually allowed to take place is the most puzzling part. It is actually quite simple because savvy thieves know the gaps in the system and how to exploit them. Today, when children are born, parents typically apply for a Social Security number for their child while still at the hospital; however, it is not until the child turns 18 and attempts to use that number to obtain credit for the first time that their number is introduced into the credit system. This leaves almost 18 years for an identity thief to create an identity for themselves with the child's Social Security number and use it undetected. Consumers do not often realize that if a credit file does not already exist for an applicant, then the credit bureaus and lenders do not check the validity of ALL information on a new credit application, only that the Social Security number was issued by the Social Security Administration. Identity thieves know this and set out to steal a child's number because it has no history linked to it. There are several ways that these thieves obtain this information.

HOW CHILD IDENTITY THEFT HAPPENS
STEP 1: STEAL A CHILD'S SOCIAL SECURITY NUMBER

- Sophisticated identity thieves create viruses specifically designed to search your computer for tax, health care, and school related documents that contain your children's Social Security numbers. Email phishing is another technique used to collect children's information.
- Data breaches and other incidences of data theft allow identity thieves to access Social Security numbers.

©2012 AllClearID. All rights reserved. No part of this publication may be used, reproduced, photocopied, transmitted or stored in any retrieval system of any nature, without the written permission of the copyright owner.

9 CREDIT CARDS

REAL-LIFE VICTIM
Brianna, 11-years-old, *Georgia*

An eleven-year-old with a mortgage, car loan and 9 credit cards. When Brianna's identity was scanned, multiple suspects and sixteen accounts associated with her Social Security number were found. The ***high balance was $132,907****. There was one* ***mortgage totaling $93,157, nine charge/credit accounts totaling $24,746****, one auto loan totaling $11,199, three installment accounts totaling $3,625 and two collection accounts totaling $180. All the activity began when Brianna was just six-years-old.*

Resolution:
AllClear ID is continuing to work the case.

- Currently, Social Security numbers are still the de facto form of national identification. As a result, a child's Social Security number is collected in a variety of places from school forms to applications for after-school activities. This allows many opportunities for a child's Social Security number to fall into the wrong hands.
- Some identity thieves predict Social Security numbers for children born after the 1990's. Though the Social Security Administration began assigning randomized numbers on June 25, 2011, numbers assigned before this date follow a pattern and can be predictable.[4]
- Children's Social Security numbers are sold everywhere from online chat rooms to flea markets. Anyone can go online and purchase an identity quickly, anonymously, and for around $40.

HOW CHILD IDENTITY THEFT HAPPENS
STEP 2: ESTABLISH A CREDIT HISTORY

Once the thief has your child's Social Security number, the next step is to establish a credit file. To do this, the thief generally tries to open accounts that have the lowest credit history requirements such as a cell phone, household utility, or an unsecured credit card. When the thief provides your child's Social Security number during the application process, he uses it with a different name and date of birth. The company or lender will run the application data through a credit bureau, but because your child's Social Security number has never been used before, there is no credit history/file to compare it against. **When a first-time credit application is received, the credit bureaus will verify the Social Security number is valid, but not the name and date of birth assigned to it when issued.** Since new Social Security numbers enter the credit world every day as new adults turn 18-years-old and consumers complete the citizenship process, a new Social Security number in the system is not seen as a suspicious event in and of itself. This initial inquiry will create a fraudulent credit header with your child's Social Security number regardless of whether the lender or service provider decides to open the account.

If the thief is able to provide a valid Social Security number (one that has been issued and is not reported as belonging to a deceased person) and the minimal identification documentation required by that lender, they are approved for the transaction and the fraudulent account is added to the credit file. This can happen because there is no widely adopted mechanism that allows a company, service provider, or bank to verify the real name and date of birth that is linked to a Social Security number. Identity thieves know about this gap in the system and depend on it to steal and use a child's Social Security number.

©2012 AllClearID. All rights reserved. No part of this publication may be used, reproduced, photocopied, transmitted or stored in any retrieval system of any nature, without the written permission of the copyright owner.

HOW CHILD IDENTITY THEFT HAPPENS
STEP 3: BUILD UP CREDIT AND DEBT, THEN DISAPPEAR

After setting up one account using your child's personal information, the thief can now go on to set up higher value accounts as he builds credit, increasing the size and complexity of the accounts as he goes. It is not uncommon to see a thief take out a loan to pay off another loan, all the while building credit and qualifying for higher amounts. This continues until the thief is ready to "cash out" and leaves all the open accounts to default into collections.

THREE IDENTITY THIEVES
33 ACCOUNTS

REAL-LIFE VICTIM
Makenna, 8-years-old, *Texas*

Health insurance coverage denied. *When Makenna's parents applied for insurance benefits for her, they were told that she was not eligible to be covered as a child because she had a work history linked to her Social Security number. It turns out that* ***three identity thieves had been using Makenna's Social Security number since she was six-years-old with a total of 33 accounts between them.*** *The cumulative high balance was $39,330 with $12,159 still appearing as debt. There were also nine accounts in collection totaling $3,784, ten installment accounts totaling $22,838, 13 credit/charge accounts totaling $12,049, and a car loan totaling $659.*

Resolution:
AllClear ID is still investigating the case.

It's important to note that in some cases, a child's Social Security number is used by someone else, not because of fraud, but because it is accidentally associated with another person's personal or credit information. For example, someone inadvertently enters the wrong numbers on an application or a creditor or credit bureau makes a data error. However, though the intent is not fraud, the impact on the child could be just as devastating because her Social Security number is associated with another person potentially blocking him or her as a young adult.

IDENTIFYING THE THIEVES

Who is committing these crimes? And what are their motives?

- Identity theft is committed by financially motivated individuals who have the opportunity to get and use the information. They also have the ability to rationalize their criminal behavior with such thoughts as, "It's really a victimless crime because the banks incur the financial loss. I'm not actually hurting anyone". These individuals understand how the system works and know how to exploit it. Often times the thief destroyed his own credit or does not have a valid Social Security number.
- Organized crime is also responsible for child identity theft. These sophisticated criminal organizations make money stealing and selling consumers' personal information. One example is illegal immigration where there is money to be made in providing those in the country illegally with Social Security numbers so they can obtain identification and employment. Here, not only is a child's identity stolen, but it is often resold to multiple people. The result is several individuals using one child's Social Security number.
- Family members may also use a child's information fraudulently to obtain credit. This generally occurs because this family member is experiencing financial hardship and/or has a bad credit history himself. Often times the goal is not to steal the child's identity and hurt the child but, though the motivation is different than that of a traditional thief, this is still fraud.

©2012 AllClearID. All rights reserved. No part of this publication may be used, reproduced, photocopied, transmitted or stored in any retrieval system of any nature, without the written permission of the copyright owner.

SEPARATING FACT FROM FICTION

Last year's Child Identity Theft Report 2011 was the first to quantify the crime and it generated significant consumer and regulatory attention to the problem. However, despite good intentions, some of the leading advice on what parents should do to detect this crime has been and continues to be incorrect.

Myth:
Checking your child's credit report is a good way to detect if your child is a victim of identity theft.
Truth:
Requesting a copy of your child's credit report will not detect the majority of the problems that may exist.

- When the credit bureaus receive a request for a credit file, they search for a match on the name plus the date of birth plus the Social Security number. This will not allow them to detect and report back to the parent cases where the child's Social Security number has been found associated with another name and date of birth.
- Unfortunately, the response that no credit file exists for their child gives parents a false sense of security and potentially an inaccurate understanding of their child's risk and what problems may already be occurring.

Myth:
Child identity theft does not impact your child's credit because often the name and date of birth linked to his Social Security number is different.
Truth:
There are several reasons why this is not true:

- Victims of child identity theft often discover this crime when they are turned down for a student loan, internship/job, apartment lease, cell phone contract, credit card, etc. While your child may not be responsible for the debts accumulated by the identity thief because the banks typically take on these losses, your child has missed an opportunity for that job, apartment, loan etc. You can work to clear up his or her credit, but in the meantime that job, apartment, or loan is gone or on hold until you do so.
- While credit bureaus allow more than one name to be linked to a Social Security number that is not the case for employers, banks, and service providers like cell phone companies. Most companies treat SSNs as unique identifiers and their systems will reject duplicates. So when your child turns 18-years-old and tries to get a job, a mobile phone, or establish credit with one of these companies, they can be blocked from doing so because that company or bank already has an identity linked to their Social Security number.

©2012 AllClearID. All rights reserved. No part of this publication may be used, reproduced, photocopied, transmitted or stored in any retrieval system of any nature, without the written permission of the copyright owner.

Myth:
Child identity theft affects only the child.
Truth:
As a parent or guardian, it is often your time, energy, and money spent working to clear up misunderstandings and restore your child's credit. Many victims refer to this process as a full-time job, one that can often be confusing, frustrating, and emotionally draining. Also, the longer a case continues the more complex it is to rectify.

Myth:
Identity theft is only a financial crime.
Truth:
Identity thieves also use children's Social Security numbers to obtain employment and, in some cases, when they are being processed for committing another crime. If your child applies for a job or internship and his or her background is checked, something like a criminal conviction can show up and ruin his or her chances. Eventually the fraudulent records will be removed, but that takes time, and it is likely the job or internship will have already gone to someone else.

CLASSIFIED "UNEMPLOYABLE"

REAL-LIFE VICTIM
Lindsey, 19 years-old, *Texas*

Restoring her identity was like a full-time job. Lindsey applied for her "dream" internship during college. A background check revealed that ***someone was using her Social Security number for employment*** *and had been doing so for many years. Lindsey was classified as "unemployable" because she did not have her "own" Social Security number. She spent months doing paperwork, standing in lines, and working with credit bureaus and the Social Security Administration trying to remedy this situation. During this time the internship was awarded to another applicant.*

Resolution:
Lindsey's identity was restored and she was able to accept the internship months later.

PROGRESS HAS BEEN MADE... BUT MORE SOLUTIONS ARE REQUIRED

Since Child Identity Theft 2011, the first large child identity theft report ever published, more attention has been paid to the problem of child identity theft.

- The Social Security Administration implemented a system of more randomized Social Security numbers. This went into effect as of June 25, 2011. Though this change may help reduce ID theft by making it harder for criminals to predict Social Security numbers, it does not address the gap that exists where credit bureaus do not verify with the Social Security Administration the name and date of birth that a Social Security number was issued to directly. It is too early to tell if this will be effective at reducing identity theft but some worry that this may actually make it *harder* for credit bureaus to notice suspicious activity and inquiries. This is because credit bureaus use this assignment logic to infer certain things about a Social Security number entering their system. Numbers issued after June 25th will actually be telling the credit bureaus less data; data that they had previously been able to make issue date and location assumptions from. This data played a role in flagging some transactions as suspicious.
- Government groups at the federal and state level have taken note of this problem and in June of 2011 The Federal Trade Commission (FTC), the Office for Victims of Crime (OVC), and the Office of Justice Programs held a forum to discuss the issue of child identity theft. The goal was to

©2012 AllClearID. All rights reserved. No part of this publication may be used, reproduced, photocopied, transmitted or stored in any retrieval system of any nature, without the written permission of the copyright owner.

get government, business, non-profit, legal service providers, and victim advocates to explore the issue of identity theft and advise parents and victims on how to ward off this crime and resolve it.

- The state of Maryland is close to passing legislation that would allow parents and guardians to create and freeze credit files for their children, effectively blocking thieves from using it. This is a positive step, yet if their child is already a victim and a credit file exists with their information; it is unclear what information and steps for remediation will be returned to the parents. It is also unclear how this freeze will get "thawed" when the child is 18. This is a potential downside if the parents are required to do something for it to be removed. Also, this only helps children living in Maryland and does not address the root of the problem, which is that there is no free or widely adopted government service or centralized mechanism that allows the real name and date of birth linked to a Social Security number to be verified.

- Another positive sign of improved protection for children is the TransUnion and State of Utah Child Identity Protection Program. Here, parents would enter each child's Social Security number in a database that would alert creditors that the information belongs to a minor when a new credit application is received. Children would be part of this high-risk alert system until they turn 17-years-old.

THE BEST PROTECTION: HOW TO PROTECT YOUR CHILDREN'S IDENTITY

- **Use free solutions designed specifically to detect child identity theft.** There are a few options to check your children's identity for signs of theft, for free:

    - ***Request a free ChildScan Report from AllClear ID.*** Since 2011, AllClear ID and TransUnion have offered a free, one-time scan of your child's Social Security number, and will fix any fraud discovered for free. Learn more about this service, and sign up for your free ChildScan at www.AllClearID.com/child

    - ***Request a free Manual Social Security number search.*** Contact the credit bureaus and request this search. It is not a standard product, so be sure to state that they should check your child's Social Security number only *(standard credit reports fail to detect 99% of child identity theft cases)*.

- **Guard their Social Security number**. Today, most hospitals have you apply for your child's Social Security number when you are filling out other documents like application for the birth certificate. Once you receive this card, typically a few weeks after your baby is born, store it in a fireproof safe at home or safe deposit box. Do not share this number or write it down and store it in places that others can easily access it. Additionally, shred any documents that may have this or other personal information belonging to your child, like insurance forms.

©2012 AllClearID. All rights reserved. No part of this publication may be used, reproduced, photocopied, transmitted or stored in any retrieval system of any nature, without the written permission of the copyright owner.

- **Start young.** Parents are commonly told to check their child's credit record around the time that the child turn 16-years-old. However, our data and victims' experiences show that this is a real problem for children at a much earlier age. It is crucial to check your child's identity as soon as you get that Social Security card and take steps to prevent the theft from occurring in the first place.

- **Go beyond the credit report. Our data showed that 41% of the fraudulent activity was occurring at sources other than the credit bureaus.** Credit reports only check for financial misuse of your child's Social Security number and only if the thief is using it with your child's specific name and specific date of birth, which is less common. This is why this is not an effective indicator of child identity theft. Credit reports will not detect cases where the thief has used your child's Social Security number for non-financial purposes, such as employment, and criminal arrests. AllClear ID searches hundreds of employment, and criminal databases for misuse with only a child's Social Security number. These data sources are generally not included in the credit bureau databases and would not be reported as part of a credit report.

- **Get anti-virus software updates.** This prevents identity thieves from getting into your computer and accessing tax, health, and school documents that may contain your child's sensitive personal information. Also, only open and download content from sources that you trust. Sites that claim to share media content like movies and music often contain harmful viruses that can infect your home computer.

- **Talk to your children about online privacy and information security.** As your children get older and begins to go online, teach them not to give out personal information like his date of birth, name, etc. Your children should also be cautious when opening or downloading content from unknown sources.

- **Use social media with caution.** Posting pictures and information on social media sites can actually make your children more vulnerable to identity theft because personal information like names, birthdays, and hometowns are revealed. Your children should be advised not to use this kind of "easy to guess" data as passwords or password hints. Research reveals that people who upload new photos of children and other family members experience fraud at a higher rate than the general population.

©2012 AllClearID. All rights reserved. No part of this publication may be used, reproduced, photocopied, transmitted or stored in any retrieval system of any nature, without the written permission of the copyright owner.

CONCLUSION

Child identity theft is a serious problem impacting the lives of many children and young adults today. Its insidious nature can result in extensive financial losses and an extremely complicated and time consuming recovery. As a result, someone else's deceit and fraud can delay important steps toward independence for your child. Child Identity Theft 2012 reveals almost 3,000 cases, each with different details, but all with financial and emotional consequences for these children and their families.

ONE-YEAR-OLD VICTIM

REAL-LIFE VICTIM
Nia, three-years-old, *California*

Nia became a victim of identity theft when she was just one year old. At mere three-years of age, Nia had three installment ***accounts totaling $2,557,*** *and two collections accounts totaling $1,660.*

Resolution:
AllClear ID removed the fraud and closed the case.

This report highlights real risks and threats and important steps that need to be taken. These include:

- 10.7% is a significant rate and alarmingly higher than the 0.3% rate of adult identity theft.
- Identity thieves are targeting young children, which means that the theft goes on longer and the damage has the potential to be more severe.
- It is critical that we raise awareness of this issue among parents. Although most parents are well aware of threats like cyber bullying, sexting, and online predators, child identity theft is not on many parents' radar.
- In addition to raising awareness, we have to make it clear how parents can protect their children. Right now, many mistakenly believe a credit report is the answer, but credit reports were not designed with children in mind. Parents have to do regular Social Security scans on their children, like the free AllClear ID ChildScan, to accurately detect identity theft.
- This report also brings to light important questions that should be the subject of scientific study like the national scope of this problem and other trends. Regardless, it is clear that the public and private sector need to work together to identify stronger protections and solutions.
- In today's world, protecting your children goes beyond the confines of their physical and emotional selves. Parents must also guard their children's identities just as fiercely as they do their own. Being proactive is the only way to stay protected.

ABOUT JAMIE MAY, ALLCLEAR ID CHIEF INVESTIGATOR & VP OF CUSTOMER SERVICE, C.F.E.

Jamie May joined AllClear ID in 2007. May is responsible for overseeing the operations of nationwide call center facilities, including hundreds of support agents, fraud investigators, and multiple phone and customer resource management systems. May is a Certified Fraud Examiner with years of experience managing identity theft investigations. Under May's direction, the AllClear ID Customer Support and Investigation teams have been recognized for exemplary service,

©2012 AllClearID. All rights reserved. No part of this publication may be used, reproduced, photocopied, transmitted or stored in any retrieval system of any nature, without the written permission of the copyright owner.

maintaining an A+ rating from the Better Business Bureau. In 2012 the team was awarded 5 Stevie Award including Best Use of Technology in Customer Service, Customer Service Department of the Year, and May was recognized as Customer Service Leader of the Year. In 2011, Javelin Strategy & Research awarded the AllClear Investigators Best in Resolution.

May is a frequent speaker on the topic of child identity theft, and has presented to the Department of Justice, Federal Trade Commission, and to multiple industry groups. May is also cited as an expert on child identity theft, featured in the New York Times, on the TODAY show, and across a variety of other print and television outlets.

ABOUT ALLCLEAR ID

AllClear ID (formerly Debix) is the technology leader in identity theft protection market, and leverages deep security experience to provide the most advanced products available. Our exclusive patented network of secure phone alerts (U.S. Patent No. 7,983,979), allows customers to respond faster and more effectively to identity threats. Fortune 500 companies, universities, state and local governments, and major healthcare organizations trust AllClear ID to protect their customers, and AllClear ID has notified over 50 million consumers.

AllClear ID supports the privacy and security industry through partnerships across key organizations. Our team serves on the Identity Theft Resource Center board, on the Steering Committee of the Online Trust Alliance and as members of the International Association of Privacy Professionals.

AllClear ID maintains an A+ Better Business Bureau rating, and in 2012 was awarded 5 Stevie Awards for outstanding customer service, including Best Use of Technology in Customer Service and Customer Service Department of the Year. In 2011, the AllClear Investigation team was named "Best in Resolution" by Javelin Strategy and Research. AllClear ID is headquartered in Austin, Texas. For more information, please visit www.AllClearID.com.

[1] AllClear ID ran credit reports for 381 confirmed cases of child ID Theft. In 99% of cases the response returned was that no credit file was found.

[2] Javelin Strategy & Research, 2012 Identity Fraud Report

[3] Stolen Futures, A Forum on Child Identity Theft: http://www.ftc.gov/bcp/workshops/stolenfutures/

[4] Social Security Administration: http://socialsecurity.gov/employer/randomizationfaqs.html#whent

©2012 AllClearID. All rights reserved. No part of this publication may be used, reproduced, photocopied, transmitted or stored in any retrieval system of any nature, without the written permission of the copyright owner.