CHILD IDENTITY THEFT

New Evidence Indicates Identity Thieves are Targeting Children for Unused Social Security Numbers

By Richard Power,
Distinguished Fellow, Carnegie Mellon CyLab

Carnegie Mellon CyLab
CONFIDENCE FOR A NETWORKED WORLD

www.cylab.cmu.edu

EXECUTIVE SUMMARY

In the cyber-centric world of the 21st Century, parents have many risks and threats to ponder as they attempt to provide a safe present and a secure future for their children. Each day, a new danger seems to capture the headlines, from exposure to online predators to the cyber-bullying by schoolmates. Meanwhile, those parents are looking over their own shoulders, careful to guard against the crime of identity theft, so that they can continue to provide that safe present, and to build that secure future. Well, it just got worse.

Because, as this report suggests, it is possible that you could be quite effective at warding off online predators and cyber-bullies, as well as proving quite successful at guarding your own hard-earned good credit, only to find that your child's identity has been violated, and your family's financial and emotional well-being threatened in an almost inconceivable way.

What would you do if your child was in foreclosure on a home in another state? Wouldn't you want to know if your child had run up a huge utility bill across town?

These are not theoretical questions, these are real-life questions that the parents and guardians of children in this report have been forced to come to grips with. In Child Identity Theft, you will find a hard look at what child identity theft means, including an analysis of over 4,000 incidents of child identity theft, and the actual stories of several victims. The report also lists recommendations for preventative measures that should be taken by both public and private sector institutions, as well as protective steps for parents to take directly.

WHAT WOULD YOU DO IF YOUR **CHILD WAS IN FORECLOSURE** ON A HOME IN ANOTHER STATE?

KEY POINTS INCLUDE

1 First large child ID theft report ever published, based on identity protection scans of over 40,000 U.S. children.

2 Unused Social Security numbers are uniquely valuable as thieves can pair them with any name and birth date. This is particularly useful for illegal immigration.

3 A child's identity is a blank slate, and the probability of discovery is low, as the child will not be using it for a long period of time. Parents typically don't monitor their children's identities.

4 The potential impact on the child's future is profound; it could destroy or damage a child's ability to win approval on student loans, acquire a mobile phone, obtain a job or secure a place to live.

5 The primary drivers for such attacks are illegal immigration (e.g., to obtain false IDs for employment), organized crime (e.g., to engage in financial fraud) and friends and family (e.g., to circumvent bad credit ratings, etc.).

parents*

** typically don't monitor their children's identities*

KEY FINDINGS INCLUDE

1. 4,311 or 10.2% of the children in the report had someone else using their Social Security number – 51 times higher than the 0.2% rate for adults in the same population

2. Child IDs were used to purchase homes and automobiles, open credit card accounts, secure employment and obtain driver's licenses

3. The largest fraud ($725,000) was committed against a 16 year old girl

4. The youngest victim was five months old; 303 victims were under the age of five

4,311 or 10.2%*

** of the children in the report had someone else using their Social Security number*

METHODOLOGY

This child identity theft report is not based on survey results. It is based on identity protection scans on 42,232 children (age 18 and under) in the U.S during 2009-2010. This pool of 42,232 child identities includes everyone under 18 in a database of over 800,000 identity records.

The participants were enrolled in the Debix AllClear ID Protection Network after receiving notice that their personal information may have been compromised during a data breach. Excluded from this report were children and adults who were affected by data breaches that resulted in targeted attacks against the population.

Note: The attacks do not appear related to the data breach events. For example, 78% of the child attacks occurred prior to the data breach events. Moreover, the attack rate for the adults affected by these same data breaches is very low at 0.2% - below the national average of 1% for the general population (Source: Javelin 2010).

This is a non-scientific report. The data does not project or imply any estimate of total number of child identity theft incidents, or what percent of children's identities are stolen, or what percent of total number of identity theft incidents involve children.

What this data does is provide some disturbing evidence that identity thieves are targeting children due to the unique value of unused Social Security numbers. It highlights some serious risks and threats, and raises some serious questions that should be the subject of a scientific study, e.g., to determine the scope of the problem, and how it is trending.

what
this
data
does*

** is provide some disturbing evidence that identity thieves are targeting children due to the unique value of unused Social Security numbers.*

INTRODUCTION

OVER FOUR THOUSAND CHILDREN'S IDENTITIES VIOLATED

Identity theft is a perennial crime that has taken on new dimensions in the Information Age. It is no longer a one-on-one crime dependent upon a lost social security card or a carelessly discarded credit card receipt. Industrialized by organized cyber criminals, 21st Century identity theft is global in its reach and exhaustive in its applications. For the individual who has been victimized, 21st Century identity theft can prove devastating in its consequences.

The numbers are shifting sands.

Hundreds of millions of identities are exposed every year; tens of millions of these identities are exploited in the commission of financial fraud.

In this report, we will focus on just a few thousand of these exposed identities.

But there is something different about this handful of sand grains.

They have a common characteristic, one that is both startling and disturbing: these several thousand identities belong to children.

In 2008, Debix the provider of AllClear ID, released a small Child Identity Theft Study based on 500 cases. This follow-up report is the largest child identity theft report ever published. The data we explore in this 2011 report is based on identity scans of over 40,000 children, and the resulting investigations that uncovered over 4,000 possible cases of child identity theft.

These 4,000+ cases raise some compelling questions.

In this brief report, we will provide some context, then explore the data and its implications, and conclude with some recommendations.

HUNDREDS OF MILLIONS

OF IDENTITIES ARE EXPOSED EVERY YEAR.

IDENTITY CRISIS

In 2009, the American Bankers Association released a survey that indicated that "for the first time, more bank customers (25%) prefer to do their banking online compared to any other method. *ABA, 9-21-09*

In January 2011, Starbucks launched a mobile payment program in all U.S. company-operated stores, allowing customers to pay for in-store purchases with BlackBerrys and iPhones. *San Francisco Chronicle, 1-19-11*

The ease of use with which you can now shop online, bank online, make travel arrangements online, pay your bills online, and pursue your personal interests online, is also available to the cyber criminal.

According to the U.S. Department of Justice, an estimated 11.7 million persons, representing five percent of all persons age 16 or older in the United States, were victims of identity theft between 2006 and 2008. These 11.7 million instances resulted in total financial losses of over $17 billion. But some of the cost is not quantifiable. Cleaning up after being victimized by identity thieves can be painful and time-consuming: "An estimated 27 percent spent more than a month clearing up the problems. Victims who spent more than six months resolving the problems associated with the identity theft were more likely to report that the experience was severely distressing… Overall, about 20 percent of victims described the identity theft as severely distressing." 11.7 million persons reported identity theft victimization in 2008, *US Department of Justice, 12-16-10*

Another reliable source of data is the Identity Theft Resource Center (ITRC). Its 2010 Breach List documents 662 breaches, in which 16,167,542 identities were exposed. *Information Week, 1-4-11*

Of course, this number includes only those breaches reported by credible sources. The total number is likely higher, perhaps much higher. The ITRC report only reflects events publicly acknowledged. There are other significant events, which have gone unreported; there are also likely to be events that were not even detected. Furthermore, the ITRC total of 16,167,542 identities exposed could easily be dwarfed by a single significant event; for example, in 2009, over 130 million credit and debit card numbers were breached in the Heartland hack, and approximately 76 million U.S. military veterans records were exposed in an accidental breach involving a recycled disk drive.

The numbers are shifting sands.

But what does this handful of sand grains tell us, what are the implications of these 4,000 plus cases involving the exposure of child identity?

11.7 million

persons reported identity theft victimization in 2008

CHILDHOOD'S END

From cyber bullying to sexting to prowling predators, the Information Age has brought with it a new spectrum of risks and threats for parents to guard their children against, and now that spectrum of threats has expanded to include child identity theft.

The online experience has changed childhood, for both better and worse. It enables children to explore the life of the world, but without proper precautions, it also enables the world to explore your child's life.

Consider a random sampling of recent surveys and news stories:

"Online bullying is a problem that affects almost half of all American teens, according to the National Crime Prevention Council. In a recent survey conducted by the Cyberbullying Research Center, 20 percent of middle-school students admitted to "seriously thinking about attempting suicide" as a result of online bullying." *MSNBC, 3/9/11*

"More young children know how to play a computer game (58%) than ride a bike unaided (52%). While a quarter of young children can open a web browser window, just 20% can swim unaided. Incredibly, while over two-thirds (69%) of 2-5 year olds can operate a computer mouse, just 17% can tie their own shoelaces." *Biz Report, 1-20-11*

"More than a quarter of young people have been involved in sexting in some form, an Associated Press-MTV poll found. … Half of all young people said they have been targets of digital bullying." *Associated Press, 12-3-10*

"Four out of five children can't tell when they are talking to an adult posing as a child on the internet, according to researchers working on software to track pedophiles online." *Science Daily, 6-2-10*

"At least three Prince Edward Island teens have been contacted on Facebook by a fake talent scout promising them a career as a model in exchange for photos of themselves in lingerie, incidents that highlight the risk to children who expose their personal details online." *National Post, 1-17-11*

"A pedophile has been arrested for allegedly breaching a restraining order and contacting children on Facebook. The arrest in Adelaide has prompted a police warning to parents to talk to their children about using the Internet safely." *Adelaide Now, 12-23-10*

"High School students have sued the Lower Merion School District in Philadelphia for spying on them using their laptops' built-in cameras. School administrators activated the webcams remotely and recorded students' activities at home." *Gizmodo, 2-18-10*

Dena Haritos Tsamitis, CyLab's Director of Education, Training and Outreach, and the developer of *www.MySecureCyberspace.com*, a free educational resource on cyber security and privacy for children and their parents, commented that "With increased cyberawareness, individuals are seeking ways to secure their personal financial information more than ever before. Based on this report, it's clear they need to go further and extend that protection for their children. Parents are already struggling to handle the threats of cyberspace, including securing their own computers and talking with their children about the many risks in cyberspace from online predators to cyberbullying. The trend in child identity theft is added weight on their shoulders. Although it will be a challenge for them to manage, it is essential to safeguarding their children's futures. "

And now, to this troubling litany, add the issue of child identity theft.

A GLIMPSE INTO WHAT THE DATA REVEALS

The data examined for this report includes the identities of 42,232 minors.

Minors whose identities showed up in the wrong places ranged from infancy to 18:

- *Cases involving identities of minors 5 and under: 303*
- *Cases involving identities of minors from 6 to 10: 826*
- *Cases involving identities of minors from 11 to 14: 1212*
- *Cases involving identities of minors from 15 to 18: 1849*

Some compelling data points emerge from this handful of sand grains, including:

- *Cases with suspect name associated with a child's Social Security number (SSN): 5,497 (Note: There are many cases with more than one suspect attached to a single child's identity. Not only is the child's ID stolen, it is shared.)*
- *Cases in which child's SSN appeared in loan and credit account records: 6,948 (Note: Within each case, there can be multiple records connected to one child.)*
- *Cases in which a child's SSN appeared in utility service records: 1,767*
- *Cases in which a child's SSN appeared in records related to property assessments, deeds, mortgages and foreclosures: 537*
- *Cases in which a child's SSN appeared in driver's license records: 415*
- *Cases in which a child's SSN appeared in vehicle registration records: 235*

There is another fascinating and disturbing number that jumps out while going through the data. The child ID theft rates stand in stark contrast to adult ID theft rates from the same security breach population. 10.2% (4,311) of these 42,232 minor's Social Security numbers had loan, property, utility and other accounts associated with them. This is fifty-one (51) times higher than the 0.2% identity theft rate for adults in the same population over the same period – 633 of the 347,362 adults had someone else use their Social Security number used to commit fraud.

Are child Social Security numbers a hot commodity? Are cyber criminals and other fraudsters seeking them out? Are child IDs preferable for fraudsters?

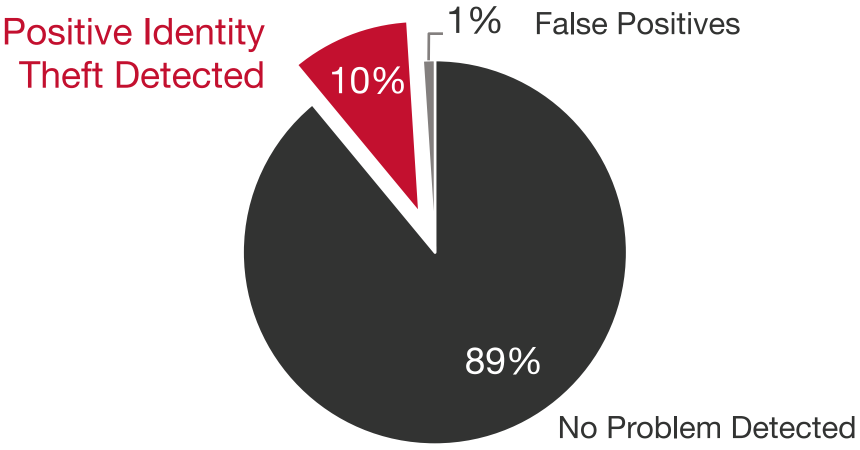
children had 51 times

higher attack rate than adults

GRAPHS & CHARTS

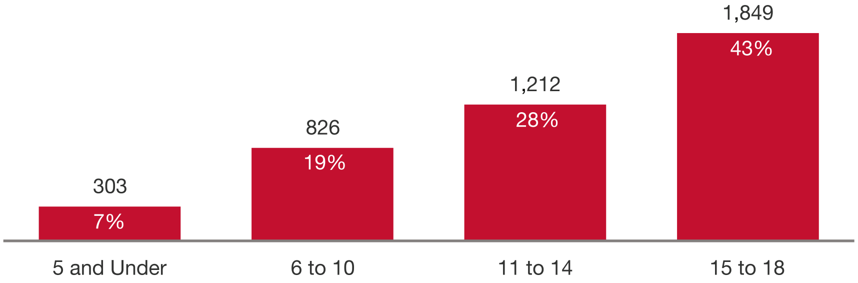
10.2% of Child Identities Scanned Exhibited Evidence of Identity Theft

Total: 42,232 Minors Identities Scanned
Time Period: 10/09 to 11/10



Age Distribution: Possible Cases of Child Identity Theft

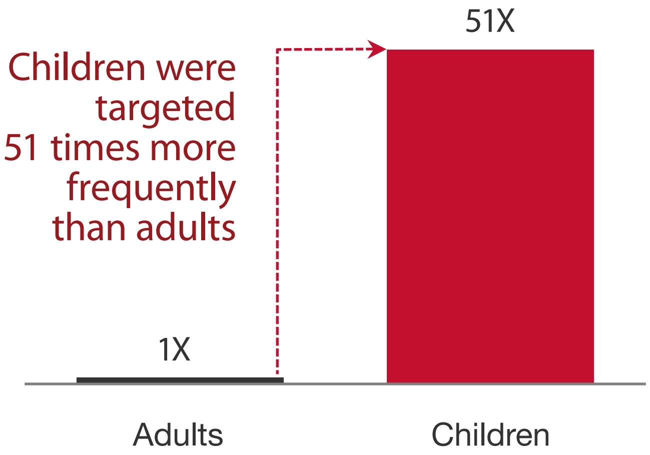
Total: 4,311 cases
Note: Age data not available on 121 children



AGE DISTRIBUTION	ACTUAL	PERCENTAGE
5 and Under	303	7%
6 to 10	826	19%
11 to 14	1,212	28%
15 to 18	1,849	43%

Rate of Child Attacks (10.2%) Vs. Rate of Adult Attacks (0.2%)

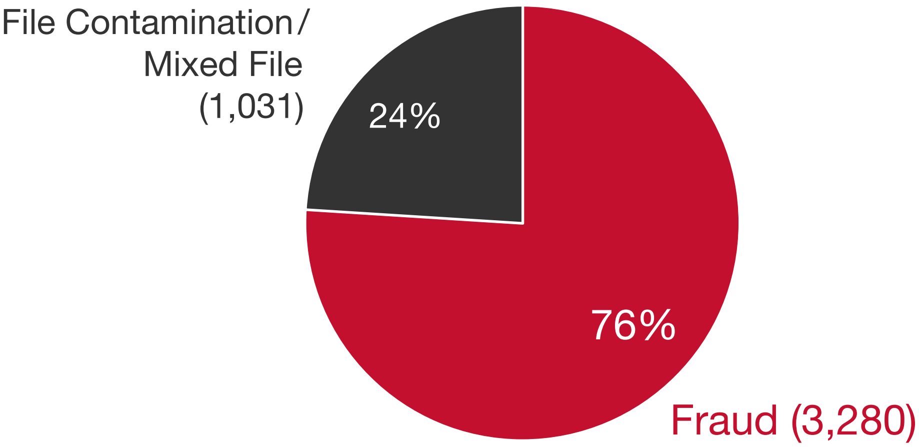
The chart to the right is based on 663 attacks against 347,362 adults and 4,311 attacks against 42,232 children, out of a total population of 351,673 (Source: Debix AllClear ID)



GRAPHS & CHARTS

Child Identity Theft Investigation Results

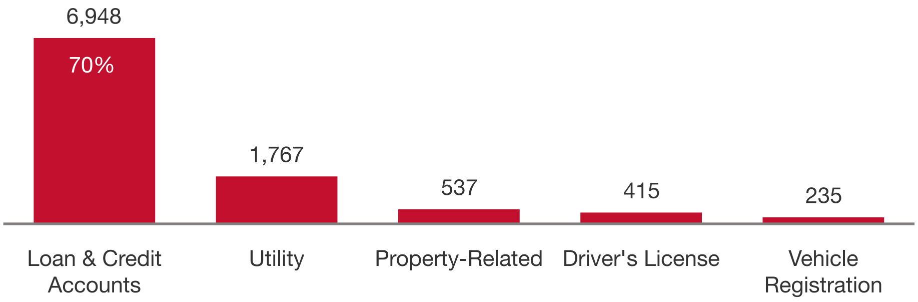
Total: 4,311
Note: File Contamination/ Mixed File indicates events caused by mistakes in reporting, not fraud. The impact to the child is the same as fraud in that the child is unable to utilize their SSN; it is assigned to someone else.



TYPE	ACTUAL	PERCENTAGE
Fraud	3,280	76%
File Contamination/Mixed File	1,031	24%

Types of Records Involved in Child Identity Theft Cases

Total: 4,311
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.



RECORD TYPE	ACTUAL	PERCENTAGE
Loan & Credit Accounts	6,948	70%
Utility	1,767	18%
Property Assessments, Deeds, Mortgages, Foreclosures	537	5%
Driver’s License	415	4%
Vehicle Registration	235	2%

IMPLICATIONS AND CONSEQUENCES

Although the data's statistical significance is yet to be determined, it is certainly profoundly significant on a practical, human level to the thousands of children and families who have thus been victimized. Furthermore, from my perspective, having tracked the evolution of cyber crime over two decades, it is only common sense to surmise that the problem goes beyond those breached accounts included in this report, and that there are many thousands more children and their families at risk.

But even if it were only one child, what if that child were yours?

Wouldn't you want to know your child was in foreclosure on a home in another state? Wouldn't you want to know if your child had run up a huge utility bill across town? Wouldn't you want to know that your child had a hunting license? Wouldn't you want to know that your child had a driver's license and a car registered in his or her name?

This AllClear ID data raises some serious questions. Wouldn't you want to know how this happened? And who was responsible? Was it the result of a security breach at a bank or a medical center or an online social media site? Was the perpetrator a petty cyber criminal or an organized cyber crime syndicate operating beyond our borders? Or was the perpetrator perhaps an insider, a family member or a close friend or a childcare worker? What recourse would you have? Where would you turn? What would the long-term consequences be for you and your child? What would it take to undo the damage done? How would you know such a crime had occurred?

The data raises broader societal questions as well. How widespread is the problem? And is it growing? What should be done governmentally? What should be done organizationally? What should be done within families? There is other evidence that child identity is an issue that demands further study.

CyLab researcher Alessandro Acquisti, co-author of the blockbuster paper, *Predicting Social Security Numbers from Public Data Proceedings of the National Academy of Science, July 7, 2009*, explains: "In our investigation of the predictability of Social Security numbers we found evidence of two trends that, combined, are particularly worrisome: criminals are increasingly targeting minors' (even infants') SSNs for identity theft, and the SSNs of younger US residents are much easier to predict than the SSNs of those born before the 1990s. Ultimately, this reminds us that our current identity-verification infrastructure is flawed and vulnerable, as it relies on authentication of numbers too widely available and too easy to compromise."

The Social Security Administration will begin assigning randomized number series http://www.ssa.gov/employer/randomizationfaqs.html as of June 25, 2011. Unfortunately, the more predictable Social Security numbers will remain in effect for individuals born before June 25, 2011.

STORIES FROM VICTIMS OF CHILD ID THEFT

The impact of child identity theft can prove substantial to both adults and children. For parents and guardians, it means a lot of time, money, and effort spent to clear the child's name. For children, if it's not discovered in time, it could mean the loss of educational and job opportunities, and starting off adulthood at a serious disadvantage – with someone else's bad credit in your name.

Here are some stories from real-life cases investigated by AllClear ID.

CHRIS FROM ARIZONA

AllClear ID discovered that a 17-year-old girl has over $725,000 in debt. Chris's daughter's Social Security number was linked to eight different suspects living in border states. The suspects opened 42 open accounts including mortgages, auto loans, credit cards, and bills in collections including medical, credit cards, and utilities.

STATUS: *The case is in progress.*

NATHAN FROM KENTUCKY

Nathan, a 14-year-old, had a credit history that went back more than 10 years. Several credit cards and a foreclosed mortgage were already in his credit history, all from a suspect living in California. The thief established good credit for the first 10 years and was able to finance a $605,000 home in CA through first and second mortgages. He also used the boy's SSN to open several credit accounts. Then, the home loans went into default and the bank foreclosed. Additionally, a credit account with over $2,000 in unpaid charges went into collections. His parents filed a police report and the fraud was assessed at over $607,000.

"I was very upset; you just don't think someone will use your child's identity," Nathan's father said. "He was only three years old when somebody started using it, and the thought of that made me sick to my stomach."

RESOLUTION: *AllClear ID has restored Nathan's identity and cleared his credit report.*

GREG FROM WASHINGTON

Greg discovered that the misuse of his 18-year-old daughter's Social Security number spanned her entire lifetime, due to an accidental transposition of some of the numbers. Although there was no malice, Greg's daughter still had a credit file using her SSN with over $325,000 in debt. This issue put their plans for college loans and scholarships in jeopardy.

Greg contacted law enforcement, but the police could not issue a complaint without a credit report. To further complicate matters, the credit agency denied Greg's request to pull a report because the owner was a minor.

"My oldest [daughter] just graduated [from college]," Greg said. "We thought this should be a piece of cake. But especially for my younger daughter, it would have been devastating if it hurt her chances of getting into college."

STORIES FROM VICTIMS OF CHILD ID THEFT

CONTINUED

RESOLUTION: *AllClear ID worked with the creditors and cleared the fraudulent accounts from the minor's file, and his daughter was able to file her student loan applications on time.*

STEPHANIE FROM IDAHO

AllClear ID discovered that Stephanie, a minor, had a credit file with unpaid debt. The suspect used Stephanie's Social Security number to open two different accounts with mobile phone companies, leaving over $1,000 in unpaid bills. The unpaid bills had moved into collections and were reported to the credit bureaus – establishing a history of bad credit for Stephanie.

RESOLUTION: *AllClear ID worked with Stephanie's parents to file police reports and restore her credit file and identity.*

GARY FROM OHIO

AllClear ID learned that 12 people living in border states were using Gary's 17-year-old son's Social Security number to obtain credit, utilities and employment. The thieves racked up over $58,000 in bad debt including a $30,000+ car, thousands in an unpaid apartment lease, and over $23,000 in unpaid credit card bills.

RESOLUTION: *AllClear ID worked with law enforcement to identify the suspects, and one was arrested and deported for using an SSN to illegally gain employment.*

LINDSEY FROM TEXAS

Lindsey applied for an internship during college, and after accepting an offer, a background check revealed someone was using her Social Security number for employment – and had been for many years – accidentally transposing some of the numbers. Lindsey was classified "unemployable" because she did not "own" her SSN. She spent months resolving issues with credit bureaus, the Social Security Administration, and her employer.

"It was like a full-time job," Lindsay recalled. "I spent hours and hours doing paperwork, standing in line, and sitting on the phone computers. I'm extremely careful now…I check my credit incessantly."

RESOLUTION: *Her identity was restored and she was able to accept the internship months later.*

BELIEVE IT OR NOT...

HERE ARE SOME STRANGER THAN FICTION FACTS EVERY PARENT SHOULD KNOW.

1 Many commercial and public sector entities do not treat Social Security numbers as unique identifiers. It is possible for one SSN to appear on more than one credit file, employment report, criminal history – all mapped to different names.

2 One reason that minor SSNs are so valuable is that there is currently no process for organizations, like an employer or creditor, to check what name and birth date is officially attached to that SSN. As long as an identity thief has a SSN with a clean history, the thief can attach any name and date of birth to it.

3 In some cases, parents can open utility bills under their child's name and SSN to take advantage of the child's clean SSN. Most parents do not intend to harm their child's future, but in fact, this is identity theft.

4 When parents opt their children out of pre-approved credit card offers, it actually creates a credit file for the minor. These files cannot be deleted once created, but can be suppressed upon request of the parent. Parents need to contact each credit bureau regarding suppressing their child's file.

5 When parents try to deal with creditors to clean up issues, the creditors can ask to speak to the child – children as young as 1-2 years old – to verify their identity. Obviously creditors don't get very far using this method!

6 Children with the same name as a parent are frequently mixed up with their parents' credit file, causing them to have to deal with their same-name parents' credit – and any related issues. Mix-ups involving names can occur for different reasons including:

- *Certain information is reported and does not contain a SSN (for example, civil judgments)*
- *Collection agencies have been known to report debts only under name and address*

7 While it is not a requirement for children to obtain SSNs, many hospitals include applying for an SSN as one of the steps for parents to complete before leaving the hospital with their newborn.

RECOMMENDATIONS

As you can see the AllClear ID data raises a lot of disturbing questions; disturbing questions for which substantive answers should be found. Therefore, my first recommendation is that this issue be the subject of academic research to learn more and better evaluate the issues involved. But whether or not these questions are answered, certain steps should be taken, because even a few thousand cases are of concern when we are dealing with the future financial security of children (and perhaps even their current safety), including:

- *Creditors and other businesses need to do a better job of authorizing accounts. There is also a known gap regarding the use of SSN as default national ID. The SSA does not share the names and date of birth with creditors and other authorizing agents, so they are left to guess that the person with the SSN is the rightful owner.*
    - *The ITRC has proposed one way for government agencies and organizations to work together would be "1710 Database" that would hold the name, Social Security number and birth month/year of every child up to the age of 17 years and 10 months. Creditors could check the database to see if credit applicants are using a minor's information. The database would be run with coordination from the Social Security Administration, state motor vehicle departments, and the three credit reporting agencies, as suggested by Jay Foley, executive director of the ITRC. The database would be of no value to marketers because it wouldn't contain addresses.*
- *Public service resources that provide guidance for individuals on identity theft prevention and mitigation, etc., should be revised and expanded to incorporate guidance on the particular issue of child identity theft and what is required of parents or guardians.*
- *Organizational strategies for dealing with the threat of identity theft among customers, employees, etc., should be revised and expanded to address the particular issue of child identity theft and what is required of the enterprise or agency to deal with the threat.*
- *Cyber security awareness and education campaigns in both the public and private sectors should incorporate information on the threat of child identity theft, and what parents and guardians need to know and do.*
- *Parents need to do cyber risk assessment for children who are, or will be going online, and develop risk mitigation plans for their online activities. Child identity theft is among numerous risks and threats that factor into the assessment. Also, just as one monitors one's own financial identity, through reviewing credit bureau reports, etc., one should monitor the SSN, etc., of any dependent minors.*

AllClear ID data raises a lot of disturbing questions*

** disturbing questions for which substantive answers should be found.*

TIPS TO PROTECT YOUR CHILD'S IDENTITY

As a parent or guardian, there are some easy steps to take to lessen the chance of your child falling victim to fraud:

- *Watch for mail in your child's name: If you begin receiving pre-approved credit cards or other unsolicited financial offers in your child's name, it is an indicator that your child may have an open credit file.*
- *Teach your child about identity theft and online safety: Talk to your child about the dangers of sharing personal data online. Children surfing the web are particularly vulnerable to exposing personal information in chat rooms or on social networking sites. Make sure children understand the importance of keeping this data private.*
- *Don't make your child susceptible to "friendly" identity theft: Don't ever use your child's name to open utility or other credit accounts. Protect your child's personal information by keeping it locked up in your home where visitors cannot access it.*
- *Keep your child's sensitive documents safe: Gauge your child's level of responsibility before you share banking and credit information with them, even accounts in their name. Most children will need their Social Security card when they go off to college, but make sure they know to keep their card in a safe place rather than carry it around in a wallet or purse.*
- *Sign up for a free service like AllClear ID that will repair your child's identity at no cost if it is stolen.*

Taking proactive measures to prevent childhood identity theft provides a sense of relief and security that cannot be underestimated. By protecting your child's identity, you are removing the potential for an enormous amount of suffering and hardship when they reach adulthood and encounter the problem on their own. Enrolling in college, beginning a career, starting a family – all become immensely difficult when your child is digging out from under the burden of restoring his or her credit history and reclaiming his or her identity.

TAKING PROACTIVE MEASURES TO PREVENT CHILDHOOD IDENTITY THEFT PROVIDES A SENSE OF RELIEF THAT **CANNOT BE UNDERESTIMATED.**

CONCLUSION

If it were only one child, it would be one too many. But this report documents over four thousand children, and there are likely many more.

This report offers disturbing evidence concerning the nature and appeal of child identity theft, and highlights some real risks and threats, e.g.:

- *10.2% is a significant rate and is dramatically higher than the attack rate for adults. Parents need to think about their children's future, and take the time to look into this frequently overlooked problem*
- *Take steps to protect your children, especially in advance of key financial milestones like student loans, college, first job, apartment rental*
- *Even though some identity theft results from non-malicious things like mixed credit files, the results are the same for parents and children. All child identity theft can result in credit, financial, and identity issues that greatly impact a child's future including school loans, job opportunities, and more*

It also raise some serious questions that should be the subject of a scientific study, e.g., to determine the scope of the problem, and how it is trending. Research needs to be conducted to quantify the scope and trending of the phenomena.

Meanwhile, institutions in both the public and private sector need to address the issue of child identity theft more aggressively.

And whether or not any action is taken on either of these fronts, parents must be proactive.

Put plainly, it is not simply enough to guard your own identity in the 21st Century, you must also guard your child's.

IF IT WERE ONLY ONE CHILD,
IT WOULD BE ONE TOO MANY.
BUT THIS REPORT DOCUMENTS
OVER FOUR THOUSAND CHILDREN,
AND THERE ARE LIKELY MANY MORE.

About CyLab

Carnegie Mellon CyLab is a bold and visionary effort, which establishes public-private partnerships to develop new technologies for measurable, secure, available, trustworthy and sustainable computing and communications systems. CyLab is a world leader in both technological research and the education of professionals in information assurance, security technology, business and policy, as well as security awareness among cyber-citizens of all ages.

Building on more than two decades of Carnegie Mellon leadership in Information Technology, CyLab is a university-wide initiative that involves over fifty faculty and one hundred graduate students from more than six different departments and schools.

Richard Power, a CyLab Distinguished Fellow, writes and speaks on cyber security. From 1995 to 2002, he directed the CSI/FBI Computer Crime and Security Survey, a widely cited study that identified several trends which have come to shape the spectrum of 21st Century cyber risks and threats.

Mr. Power is the author of Tangled Web: Tales of Digital Crime from the Shadows of Cyberspace (Que) and co-author of Secrets Stolen, Fortunes Lost: Preventing Intellectual Property Theft and Economic Espionage in the 21ST Century (Syngress).

www.cylab.cmu.edu

About AllClear ID

AllClear ID, a new product from Debix, offers free, essential identity protection to everyone. Debix is a pioneer and leading force in the identity protection industry, and using advanced technology created the world's first and only Identity Protection Network.

Fortune 500 companies, universities, state and local governments, healthcare companies, and many other national organizations use Debix to protect their customers, and Debix has protected over 1 million individuals.

Debix and AllClear ID are led by experienced and respected Executives and a renowned Advisory Board. Founded in 2004, Debix is headquartered in Austin, Texas and is privately funded.

www.AllClearID.com

Carnegie Mellon

CyLab

CONFIDENCE FOR A NETWORKED WORLD

www.cylab.cmu.edu