SB 121

<TARGET><BILL>SB 121</BILL><SUBJECT>SB 121</SUBJECT><COMM>HJUD29</COMM></TARGET>

Alaska State Legislature

Interim:
716 West 4th Avenue
Anchorage, Alaska 99501
(907) 269-0199 Phone
(907) 269-0197 Fax

Session:
State Capitol Building, Room 111
Juneau, Alaska 99801-1182
(907) 465-4945 Phone
(907) 465-3476 Fax

Senate President Kevin Meyer

Senate District M

SB 121: Security Freeze on Minor's Credit Report

SB 121 allows a parent, legal guardian, or conservator of a minor, incapacitated person or protected person, to place a security freeze on the credit report of the minor, incapacitated person or protected person, and allows for the creation of a credit file by a credit bureau in order to place if a freeze if none currently exists. Alaska statute does not specifically state that a parent or legal guardian/conservator can request a freeze on a minor's credit report, and while the credit bureaus have generally allowed parents to do so in the past, SB 121 will expressly permit this action.

According to the 2012 Child Identity Theft Report, children are 35 times more likely to be subject to identity theft than adults, increasing the possibility that a parent or the minor would not catch such a crime until reported to a collection agency, or until the individual applies for credit or financial aid. Unfortunately, clearing up fraudulent claims on a credit file can take from several months to several years, and could severely limit the options for young people just entering adulthood. The same is true for vulnerable adults that may not be able to manage their own finances and credit. They may never establish a credit file in their name, and therefore their credit is often a target for identity thieves.

SB 121 will give parents, legal guardians, and conservators a much needed tool to safeguard dependents against identity theft and financial fraud prior to the crime occurring. I respectfully request your support on SB 121.

SB 121 – "AN ACT RELATING TO A SECURITY FREEZE ON THE CONSUMER CREDIT REPORT OF A MINOR."

SUMMARY OF CHANGES

The changes below were made to add vulnerable adults who may not be able to make independent financial decisions to the legislation in order for their legal representative to request a credit freeze.

1. Page 1, Line 6: Added "or conservator of a minor, incapacitated person, or protected person..."

2. Page 1, Lines 8-9: Added "incapacitated person, or protected person under the supervision of that parent, legal guardian, or conservator."

3. Page 1, Lines 13-14, continuing through Page 2, Lines 1-5: Added definitions for "conservator," "incapacitated person" and "protected person."

Fiscal Note

State of Alaska
2016 Legislative Session

Bill Version:	SB 121
Fiscal Note Number:	1
(S) Publish Date:	1/29/2016

Identifier: SB121-LAW-CIV-01-23-16
Title: SECURITY FREEZE ON CERTAIN CREDIT REPORTS
Sponsor: MEYER
Requester: Senate Labor & Commerce

Department: Department of Law
Appropriation: Civil Division
Allocation: Commercial and Fair Business
OMB Component Number: 2717

Expenditures/Revenues

Note: Amounts do not include inflation unless otherwise noted below. (Thousands of Dollars)

	FY2017 Appropriation Requested	Included in Governor's FY2017 Request	Out-Year Cost Estimates				
OPERATING EXPENDITURES	**FY 2017**	**FY 2017**	**FY 2018**	**FY 2019**	**FY 2020**	**FY 2021**	**FY 2022**
Personal Services							
Travel							
Services							
Commodities							
Capital Outlay							
Grants & Benefits							
Miscellaneous							
Total Operating	**0.0**	**0.0**	**0.0**	**0.0**	**0.0**	**0.0**	**0.0**
Fund Source (Operating Only)							
None							
Total	**0.0**	**0.0**	**0.0**	**0.0**	**0.0**	**0.0**	**0.0**
Positions							
Full-time							
Part-time							
Temporary							
Change in Revenues							

Estimated SUPPLEMENTAL (FY2016) cost: 0.0 *(separate supplemental appropriation required)*
(discuss reasons and fund source(s) in analysis section)

Estimated CAPITAL (FY2017) cost: 0.0 *(separate capital appropriation required)*
(discuss reasons and fund source(s) in analysis section)

ASSOCIATED REGULATIONS

Does the bill direct, or will the bill result in, regulation changes adopted by your agency? No
If yes, by what date are the regulations to be adopted, amended or repealed?

Why this fiscal note differs from previous version:

Not applicable, initial version

Prepared By:	Valerie Rose, Budget Analyst	Phone:	(907)465-3674
Division:	Administrative Services Division	Date:	01/23/2016 08:24 AM
Approved By:	Craig W. Richards, Attorney General	Date:	01/23/16
Agency:	Department of Law		

FISCAL NOTE ANALYSIS

STATE OF ALASKA
2016 LEGISLATIVE SESSION

Analysis

SB 121 would add a new section, AS 45.48.220, to AS 45.48 (Personal Information Protection Act) to allow a parent or guardian of a minor to make a request under AS 45.48.100 - 45.48.290 (Credit Report and Credit Score Security Freeze) in order to place a security freeze on the minor's consumer credit report. If a consumer credit report does not exist at the time the request is made, the consumer credit reporting agency would be required to generate a record or consumer credit report for the purpose of placing a security freeze.

The Department of Law does not anticipate a fiscal impact to the department should this bill become law.

LEGAL SERVICES

DIVISION OF LEGAL AND RESEARCH SERVICES
LEGISLATIVE AFFAIRS AGENCY
STATE OF ALASKA

(907) 465-3867 or 465-2450
FAX (907) 465-2029
Mail Stop 3101

State Capitol
Juneau, Alaska 99801-1182
Deliveries to: 129 6th St., Rm. 329

MEMORANDUM October 8, 2015

SUBJECT: Security freeze on minor's credit report
(Work Order No. 29-LS1129\A)

TO: Senator Kevin Meyer
Attn: Edra Morledge

FROM: Megan A. Wallace
Legislative Counsel

Enclosed please find the draft bill you requested. While Alaska law does not expressly permit a parent or legal guardian to place a freeze on a minor's credit report, my preliminary research revealed that credit agencies will generally allow a parent to do so, provided that the minor has a credit report to freeze. Unless credit has been opened in the minor's name, or the minor has been added as an authorized user to a credit card, the minor may not have a credit report - which would prevent the credit agency from placing a freeze on the minor's credit report, because none exists. As such, this bill expressly allows parents to make a request on behalf of a minor and also requires a credit agency to generate a credit report for the purpose of placing a freeze on the minor's credit report if one does not already exist at the time of the request. If this was not your intent, please advise.

Please be advised, however, that the bill may be construed to give parents and/or minors greater protection than is provided to other adult consumers, to the extent that credit agencies are not required to generate a report for adult consumers who may not have any credit history. In this regard, please advise if you wish to include a provision that would require credit agencies to generate a credit report for all consumers who may not already have a credit report for the purpose of placing a security freeze.

MAW:dla
15-481.dla

Enclosure

Department of Law
Consumer Protection Unit

Alaska Personal Information Protection Act

House Bill 65 was passed by the Legislature during the 2007-2008 session, and became law on July 1, 2009. It is found in the Alaska Statutes at AS 45.48. The law provides several protections for personal information, including: (1) a notice requirement when a breach of security concerning personal information has occurred; (2) the ability to place a security freeze on a consumer credit report; (3) various restrictions on the use of personal information and credit information; (4) the disposal of records containing personal information; (5) allowing a victim of identity theft to petition the court for a determination of factual innocence; and (6) truncation of credit card information. These protections are contained in various sections of the statute as follows:

Sec. 45.48.010 - .090 – Breach of Security Involving Personal Information.

This article contains provisions that require notification to consumers when there is a breach of security of an information system containing personal information. "Personal information" is defined to include information on an individual, that is not encrypted, that consists of the individual's name and one or more of several other pieces of information, including a social security number, driver's license number, account number, password, or other access codes.

Notice of the breach must be done expeditiously. Notice can be delayed if it will interfere with a criminal investigation, or if the breach is unlikely to cause harm to the consumer. Notice must be given in writing, but can also be given by electronic means under certain circumstances.

Violations of this section subject the violator (including a state agency) to a civil penalty of up to $500 for each consumer who was not provided notice, up to a maximum penalty of $50,000. In addition, the injured person can seek injunctive relief, and can recover actual economic harm.

Sec. 45.48.100 - .290 – Credit Report and Credit Score Security Freeze.

This article contains provisions that allow a consumer to place a security freeze on the consumer's credit report. The effect of a freeze will prevent a third person from accessing the individual's credit report. A freeze can be placed by mail or other means if the credit reporting agency allows a freeze by another means. Once a freeze is in place, the consumer can remove it by submitting a request in a similar manner.

A credit reporting agency can charge $5 to place a freeze, and $2 to remove the freeze. Because there are currently three major credit reporting agencies, this equates to $15 and $6 respectively to place and remove a freeze at all three companies.

There are several exemptions that allow access by certain entities even when a freeze is in place, including (1) use of the credit report to review or collect a financial obligation; (2) persons acting under court order; (3) a municipal or state agency that administers child support enforcement obligations; (4) the department of Health and Social Services when investigating fraud; (5) the Department of Revenue when investigating or collecting taxes or implementing other statutory responsibilities; (6) prescreening allowed by the Fair Credit Reporting Act; and (7) for insurance purposes.

Knowing violations of this section subject the violator to actual economic damages, including punitive damages up to $5,000 for each violation.

Sec. 45.48.400 - .480 – Protection of Social Security Number.

This article contains provisions that restrict the use of social security numbers ("SSN's") in a number of ways. There are four sections that address specific uses of a SSN:

Section 45.48.400 prohibits a person from making a SSN available to the public. This section also prohibits a person from requiring a SSN to access products or services, including internet access, and prohibits the printing of a SSN on material mailed to a consumer unless required by state or federal law. The prohibitions of the section do not apply to government agencies if use of the SSN is authorized by law or required for the performance of the person's duties or responsibilities as provided by law.

Section 45.48.410 prohibits the request and collection of SSN's. The prohibition on the request or collection does not apply:

1. if the person is authorized by law to request or collect a SSN;
2. to a government agency if the agency is authorized by law to request or collect the SSN, or the request or collection is required for the performance of the person's duties or responsibilities as provided by law;
3. to a person subject to the Gramm-Leach-Bliley Act;
4. to a person subject to the Fair Credit Reporting Act;
5. if the request or collection is for a background check, law enforcement, employment, or verifying a person's age;
6. if the request or collection is part of a larger transaction and does not have independent economic value;
7. to an insurer regulated by AS 21; or
8. to a hospital/medical service corporation regulated by AS 21.87.

Section 45.48.420 prohibits the sale, lease, loan, or trade of a SSN unless the sale, lease, loan, or trade is:

1. authorized by law;
2. by a person subject to the Gramm-Leach-Bliley Act;
3. by a person subject to the Fair Credit Reporting Act; or

4. part of a report prepared by a consumer reporting agency in response to a request by a person who submits the SSN as part of the request.

Knowing violations of the section are a class A misdemeanor.

Section 45.48.430 prohibits the disclosure of a SSN, unless the disclosure:

1. is authorized by law;
2. is by a government agency and the disclosure is required for the performance of the person's duties;
3. is to a person subject to the Gramm-Leach-Bliley Act;
4. is to a person subject to the Fair Credit Reporting Act;
5. is part of a report prepared by a consumer reporting agency in response to a request by a person who submits the SSN as part of the request; or
6. is for a background check, identity verification, fraud prevention, medical treatment, law enforcement, or employment.

Other sections of Article 3 allows for the interagency disclosure of a SSN, and use by employers when administrating a claim, benefit or procedure related to the individual's employment. A person may also disclose a SSN to an employee or agent of the person for legitimate purposes directed by the person.

Knowing violations of AS 45.48.400 - .430 are subject to a $3,000 penalty plus actual economic damages, court costs, and full reasonable attorneys fees.

Sec. 45.48.500 - .590 – Disposal of Records

This article contains provisions that require a business and a government agency to take reasonable measures to protect against unauthorized access to, or use of, records when disposing of records containing personal information. To comply with this requirement, a business or government agency can implement compliance and monitoring policies that require the destruction of personal information, or enter a contract with a third party for the disposal and destruction of the records. A business or government agency is not liable for the disposal after relinquishing control of the records to a third party that is in the business of record destruction.

Knowing violations of this section are subject to a $3,000 penalty plus actual economic damages, court costs, and full reasonable attorneys fees.

Sec. 45.48.600 - .690 – Factual Declaration of Innocence After Identity Theft; Right to File Police Report.

This article contains provisions that allow a victim of identity theft to petition the Alaska Superior Court for a declaration that the individual is factually innocent of the crime if the perpetrator was arrested, cited, or convicted of the crime. The court has broad discretion to make a determination based on declarations, affidavits, or other relevant material. This section also allows the Department of Law to establish and maintain a database of

individuals who have been the victims of identity theft and who have been declared innocent of the crime.

There is also a provision that allows a person who has learned or reasonable suspects that she has been the victim of identity theft to file a police report with the local law enforcement agency, even if the agency does not have jurisdiction over the identity theft.

Sec. 45.48.750 – Truncation of Card Information.

This article contains provisions that prohibit the printing of more than the last four digits of a credit or debit card number on any receipt provided at the point of sale. In addition, a person may not sell a device that electronically prints more than the last four digits of a credit or debit card.

Knowing violations of this section are subject to a $3,000 penalty plus actual economic damages, court costs, and full reasonable attorneys fees.

For a full text of the law, visit the Alaska State Legislature's infobase under 2008 Alaska Statute 45.48

Department of Law attorney.general@alaska.gov P.O. Box 110300, Juneau, AK 99811-0300
Phone: 907-465-3600 Fax: 907-465-2075 TTY: 907-258-9161

From: Hughes, Laura [mailto:lj_ak@yahoo.com]
Sent: Thursday, May 28, 2015 10:05 AM
To: Sen. Kevin Meyer
Subject: Dear Senator Kevin Meyer,

Senator.Kevin.Meyer@akleg.gov

Dear Senator Kevin Meyer,

Hello, my name is Laura Hughes. I am a South-Anchorage resident in your district, District M. I am writing to ask for your assistance in passing legislation that would protect the credit of children/minors in the state of Alaska.

Currently in Alaska, a parent or guardian cannot request that a credit report for a minor under the age of 18 be frozen unless that child's credit has actually been stolen or used inappropriately.

Children are increasingly more likely to have identities stolen as a result of this age gap where no protection is afforded. According to the 2012 Child Identity Theft Report, children are 35 times more likely to be subject to identity theft than adults.

This increases the probability that a parent or the minor would not catch such a crime until reported to a collection agency, or until the individual applied for some sort of credit or financial aid. As a result, a minor may turn 18 and unfortunately have to deal with this problem after requesting a report from the three major credit bureaus (Equifax, Experian, TransUnion).

Clearing up fraudulent claims on a credit file can take from several months to several years, and it can also create undue stress for the individual that is the victim of identity theft.

Currently the credit bureaus offer "credit monitoring services" that in reality provide no protection against identity theft, and are a product solely for generating revenue for these companies that hold information vital to fiscal development of everyone's lives. The credit bureaus generate revenue by selling people's credit history to bidders.

It is in their financial interest to keep people in monitoring programs because once credit is frozen, they may not share information in credit files as freely. In addition, the three credit bureaus continually use strong-arm tactics and lobby against such legislation being passed.

In increasingly partisan atmospheres that persist across all levels of government, I feel that protecting the credit of children is an item of legislation that would cross both aisles. It would also be a great boost for representatives who help sponsor and pass such legislation as advocates of the common voter in Alaska.

As a parent of two young children, I worry often that we may find that someone could have tampered with or accessed their credit when they turn 18. This may severely limit their options if they were to try to apply financial aid for college, in addition to other financial decisions they may try to execute.

In addition, the sad truth of identity theft for children is that much of it is due to unscrupulous activity of a dishonest family member who may be in dire financial straits.

The states of Delaware, Georgia, Florida, Hawaii, Illinois, Maine, Maryland, Massachusetts, Michigan, Minnesota, and Texas have all recently passed or are in process of passing legislation giving parents or guardians the ability to protect their children at birth. Please help the children of Alaska do the same with sensible legislation. I would be willing to assist with this effort as a vocal advocate if it would help move this agenda forward.

Thank you very much for your time and support of the Anchorage and Alaska communities.

Sincerely,

Laura Hughes
11322 Forest Drive

Anchorage, AK 99516
LJ_AK@yahoo.com
(907)952-0367

NATIONAL CONFERENCE of STATE LEGISLATURES

Identity Theft Strikes Young

5/22/2014

STATE LEGISLATURES MAGAZINE | JUNE 2014

Identity thieves are targeting children who may not even discover they've had their personalinformation stolen for several years.

By Heather Morton

The stories of children falling victim to identity theft are growing at an alarming rate. A college freshman starts receiv court summonses stemming from large, unpaid credit card bills tracked to her. The cards were made with her Social Security number, but without her knowledge, when she was only 13.

A parent applies for Medicaid and discovers during the application process that someone been using her 5-year-old son's Social Security number in employment applications sinc was born.

A young couple tries to buy a first home, but the woman's credit score disqualifies them. then does she discover that her mother used her Social Security number to purchase a c and a mortgage following a nasty divorce that badly damaged her credit rating. The daug had to decide whether to report her mother to the police in order to clean up her identity.

These cases, and many others like them, are happening to children with increasing frequency. Although identity theft has been the No. 1 consumer complaint received by the Federal Trade Commissio the last 14 years, identity thieves targeting very young victims is a relatively new concern. "As someone who was the victim of identity theft more than 10 years ago, I fully understand the devastating effect such a crime can have on a person's short- and long-term financial standing," says Pennsylvania Representative Matthew Baker (R).

"The crime is especially heinous when perpetrated using the identity of a child, who often doesn't know his or her ide has been stolen until many years after the fact, when he or she first applies for college assistance or a credit card. Tl can lead to lifelong financial headaches and delayed enrollment in college until the situation can be resolved."

A Relatively Young Crime

Identity theft is generally defined as: The use of a person's personally identifying information—a name, Social Secun number, credit card number or other financial information—without permission, to commit fraud, theft or other crimes

After the enactment of the federal Identity Theft and Assumption Deterrence Act of 1998, the Federal Trade Commis created the Consumer Sentinel Network to collect consumers' complaints to share with law enforcement personnel. ' secure, online database has since collected millions of complaints involving fraud and identity theft.

Every state now has a law regarding identity theft or impersonation. Twenty-nine states, the District of Columbia, Gu and Puerto Rico have specific restitution provisions for identity theft that require thieves to reimburse victims. Five states—Iowa, Kansas, Kentucky, Michigan and Tennessee—have forfeiture provisions.

Despite the laws, identity thieves continue to succeed at finding easy victims. And when they do, they can cause a lc damage. In a recent survey by the Bureau of Justice Statistics, victims reported losing a total of $24.7 billion in direct

indirect costs because of identity theft in 2012. In fact, losses from identity theft exceeded the $14 billion in losses reported from all the other property crimes—burglary, theft and motor vehicle theft—combined.

Why Target Kids?

Among the 13 million consumers whose identities were stolen in 2013, are a growing number of children. One in 40 families with children under 18 had at least one child whose personal information was compromised, according to a : survey by the Identity Theft Assistance Center and the Javelin Strategy & Research group. The survey revealed that identity thieves most often steal children's Social Security numbers, since young children seldom have the credit hist acquired by adults, such as credit cards, bank accounts, licenses and financial statements.

Nevertheless, children's identifying information is very appealing to thieves who will often create "synthetic" identities using a child's Social Security number with a different date of birth to avoid detection.

Most children have no credit histories and their Social Security numbers have not yet been flagged in any fraud prevention database. Unmarked and untested, children's stolen identities often go unnoticed until after they reach 18 This allows the fraud to continue for years. In the 2012 Identity Theft Assistance Center/Javelin Child Identity Fraud Survey, 17 percent of children were victimized for a year or longer.

Clearing one's name and securing one's real identity also can take years.

Aston Betz-Hamilton, the college student who received numerous court summonses, spent 16 years trying to repair i credit report. Although she was relieved when the last of the fraudulent entries finally dropped off her credit report in 2009, a few years later she was devastated when she learned her mother had been the thief.

With easy access to official documents, family members and their friends often are the thieves. Parents know the da birth and usually share the same name. When a parent's credit is poor or a guardian's felony conviction prevents hin from finding a job, using the child's identity is just too easy for some. And young victims face quite a challenge if aske turn in their own parents.

Twenty-seven percent of the Identity Theft Assistance Center/Javelin survey respondents reported knowing the individual responsible for the crime, complicating family dynamics and friendships. Ana Ramirez, whose mother usec Social Security number when Ana was 10, chose not to file a police report out of loyalty to her mother

Lawmakers Respond

In response to this growing problem, state legislators have strengthened criminal penalties, required credit reports fo children in the foster care system, and allowed parents and guardians to request consumer report security freezes o behalf of their children.

Lawmakers in Florida, Indiana, Louisiana and Pennsylvania have increased criminal penalties if the victim is a minor Florida, a person who fraudulently uses a minor's personal identification information now faces a second-degree felo charge, while criminal use of an adult's personal identification information remains punishable as a third-degree felor

In 2009, Indiana legislators enhanced the penalty for the crime of "identity deception" from a class 6 felony to a class felony if a person uses identifying information from a son, daughter, ward or other dependent.

"As we move deeper into the information age, identity theft becomes easier and more prevalent, leaving thousands c Hoosiers at risk of losing their good financial standing to unscrupulous criminals," says Indiana Representative Linda Lawson (D). "It is our duty to protect Hoosiers from these deceptive acts."

In Louisiana, lawmakers decided to set minimum sentencing times for identity theft committed against a child under a 17, depending on the monetary value associated with the crime.

In Florida and Pennsylvania, lawmakers chose to increase the criminal penalty by one grade if a person steals the identity of a child under age 18.In the definitions of what constitutes the crime of identity theft, Georgia and Texas specifically added using the identifying information of an individual under 18.

In Kentucky, state legislators included in the state's identity theft statute possessing or using current or former identif information of a family member.

The Power to Freeze Credit Reports

Forty-nine states and the District of Columbia allow consumers to place a "security freeze" on their credit report to lin reporting agency from releasing a report or any information from it without authorization from the consumer. The sec freeze is designed to help prevent identity thieves from opening new accounts using the victim's identifying informati

Now, legislators are making this tool available to children to prevent identity theft. Thirteen states have expanded the to allow a parent or guardian to place a security freeze on a minor's consumer credit report. Other states are conside similar measures.

"This crime can have a devastating effect on an individual's personal finances, and we should ensure that our young people can begin their adult lives with a clean financial slate," says Senator Jane Nelson (R), who sponsored the legislation in Texas.

"By allowing parents to place a 'Do Not Enter' sign on their child's credit record, this legislation will help protect youn Texans from identity theft."

Identity theft can wreak havoc on an individual's life, requiring many hours and lots of paperwork to resolve. Brittany Marston spent three years writing letters, making telephone calls and finally threatening to involve an attorney in ord remove the credit card charges and fees from her credit report that she discovered when she turned 18. For children impact can be even more devastating, particularly if the identity theft has been perpetrated by a family member.

Although state legislation cannot prevent all cases of identity theft, state legislators are giving children and their pare some new tools to combat the problem if they are victimized.

Foster Care Concerns

Statistics on identify theft among foster children specifically are difficult to find. For example, a 2011 pilot project in California found that although accounts had been opened in the names of 5 percent of 2,110 foster children in Los Angeles County, there was no way to confirm why the accounts were opened. Nevertheless, it is widely believed tha children in the foster care system are more vulnerable to identity theft than other kids for a couple of reasons.

First, the identities of children in foster care are more easily compromised by family members without the children's knowledge, since they are separated. Second, the personal identifying information and sensitive health information c foster care children often are shared throughout the social services system and are available to a greater number an variety of people.

Anecdotal evidence supports a reason for concern. When Suamhirs Rivera, for example, left the foster care system a age 18, he discovered that someone had used his identity while he was in foster care to charge more than $75,000. four years, Rivera has been able to clear only $35,000 of the fraudulent charges from his credit record, and he still fa two lawsuits for fraud. He continues to work to clear the remaining $40,000.

"It has been difficult to resolve my credit problems, especially because I have no support from anyone—no family in t United States and no one to back me up," Rivera says. "Young people should know about bad credit long before the leave care."

Recognizing that children in the foster care system may need a little extra help to determine if their personal informat has been misused, state and federal policymakers now require child welfare agencies to obtain and examine credit reports of all children in the system as they approach their 16th birthdays.

"Unfortunately, identity theft among foster youth usually isn't discovered until after they have 'aged out' of the foster c system and have lost the resources and support needed to fix the problems," says District of Columbia Councilmemt Tommy Wells (D). "For these youth, adulthood will begin with credit histories that are tarnished through no fault of th own."

After 2006, when California, Colorado, Connecticut, Illinois, Texas and the District of Columbia enacted legislation, Congress followed with the Child and Family Services Improvement and Innovation Act of 2011, mandating that all children in foster care, starting at age 16, receive a free consumer report each year until they leave the foster care system and any assistance they need to interpret and resolve any inaccuracies in the report.

Following the 2011 congressional action, Delaware, Nevada and Virginia enacted similar state legislation.

Heather Morton tracks financial services, civil liability and alcohol regulation for NCSL.

Five Common Warning Signs

Identity theft can be hard to detect, although these warning signs should raise reds flags immediately.

1. A family receives calls from collection agencies, bills from credit card companies or medical providers, or offers fo credit cards or bank account checks in a child's name, even if the child has never applied for or used these services.

2. A child or a family is denied government benefits because another account using that Social Security number is already receiving benefits.

3. The Social Security Administration, Internal Revenue Service or some other government agency asks to confirm t child is employed, even though the child has never had a job.

4. The IRS notifies a parent that the same information he or she filed for a dependent child is listed on another tax re

5. A child receives a notice from the IRS saying he or she failed to pay taxes on income the child has never received

Source: Federal Trade Commi

Have You Checked Your Credit Report?

The federal Fair Credit Reporting Act requires each of the nationwide credit reporting companies—Equifax, Experian TransUnion—to provide consumers over age 18 with a free copy of their credit report, upon request, once every 12 months. The website, www.annualcreditreport.com, is the only one authorized to fill orders for a free report, although consumers may also call 1-877-322-8228 to request a report.

Callers will need to provide their name, address, Social Security number, and date of birth. If they have moved in the two years, they may have to provide their previous address. To maintain security, the credit reporting agencies may for some personal information, such as the amount of a monthly mortgage payment. Each company may ask for diff information because the information each has comes from different sources.

For children younger than 18, parents, legal guardians and child welfare agencies must request a manual search of child's credit file through a written request directly to each consumer reporting agency. The credit reporting companie may require copies of:

- The child's birth certificate and Social Security card
- The parent's driver's license or military identification,

- Proof of address, such as a utility bill or credit card statement, and
- Copies of documents proving legal guardianship of the child.

Additional Resources

NCSL Resources

- Subscribe to State Legislatures
- State Legislatures homepage

Other Resources

- Child Identity Theft | **Federal Trade Commission**
- 2012 Child Identity Fraud Report | **Identity Theft Assistance Center**
- Victims of Identity Theft, 2012 | **Bureau of Justice Statistics**
- 2013 Identity Fraud report | **Javelin Strategy and Research**
- ITRC Fact Sheet 120 Identity Theft and Children | **Identity Theft Resource Center**

NATIONAL CONFERENCE of STATE LEGISLATURES

Consumer Report Security Freeze State Laws

12/17/2015 Heather M

Fifty states and the District of Columbia have enacted legislation allowing consumers to place "security freeze" on th credit reports. A consumer report security freezes limits a consumer reporting agency from releasing a credit report c any information from the report without authorization from the consumer. If a person suspects that he or she has bee victimized by identity theft, a consumer report security freeze can help the person track whether an identity thief is us the person's information to set up bogus accounts.

Twenty-three states allow parents, legal guardians or other representatives of minors to place a security freeze on th minor's credit report.

SECURITY FREEZE LAWS

State	Citation	Who May Request a Freeze
Alabama	Ala. Code §8-35-1 *et seq.*	Any consumer
Alaska	Alaska Stat. §45.48.100 *et seq.*	Any consumer
Arizona	Ariz. Rev. Stat. Ann. §44-1698 2015 Chapter 280	Any consumer, including a representative of a "protected person," meaning an individual who is under 16 years o at the time a request for the placement of a security freeze is made or who is an incapacitated person or a protect person for whom a guardian or conservator has been appointed.
Arkansas	Ark. Stat. Ann. §4-112-101 *et seq.*	Any consumer
California	Cal. Civil Code §1785.11.2 *et seq.*	Any consumer
Colorado	Colo. Rev. Stat. §12-14.3-101 *et seq.*	Any consumer
Connecticut	Conn. Gen. Stat. §36a-701 *et seq.* 2015 Public Act 62	Any consumer, including a parent or legal guardian of a minor child. Minor child means an individual under 18 yea age at the time a request for placement of a security freeze is submitted.
Delaware	Del. Code Ann. tit. 6, §2201 *et seq.*	Any consumer, including a representative of a "protected consumer," an individual who is: a. Under the age of 16 at the time a request for the placement of a security freeze is made; or b. An incapacitated person or a protected p for whom a guardian or conservator has been appointed.
District of Columbia	D.C. Code Ann. §28-3861 *et seq.*	Any consumer
Florida	Fla. Stat. §501.005 and §501.0051	Any consumer, including a representative of a "protected consumer," a person younger than 16 years of age at th a security freeze request is made or a person represented by a guardian or other advocate pursuant to chapter 3(chapter 393, chapter 744, or chapter 914.
Georgia	Ga. Code §10-1-913 *et seq.*	Any consumer residing in the state, including a representative of a "protected consumer," an individual who is: (A Under the age of 16 years at the time a request for the placement of a security freeze is made under subsection ((Code §10-1-914.1; or (B) An individual for whom a guardian or conservator has been appointed.

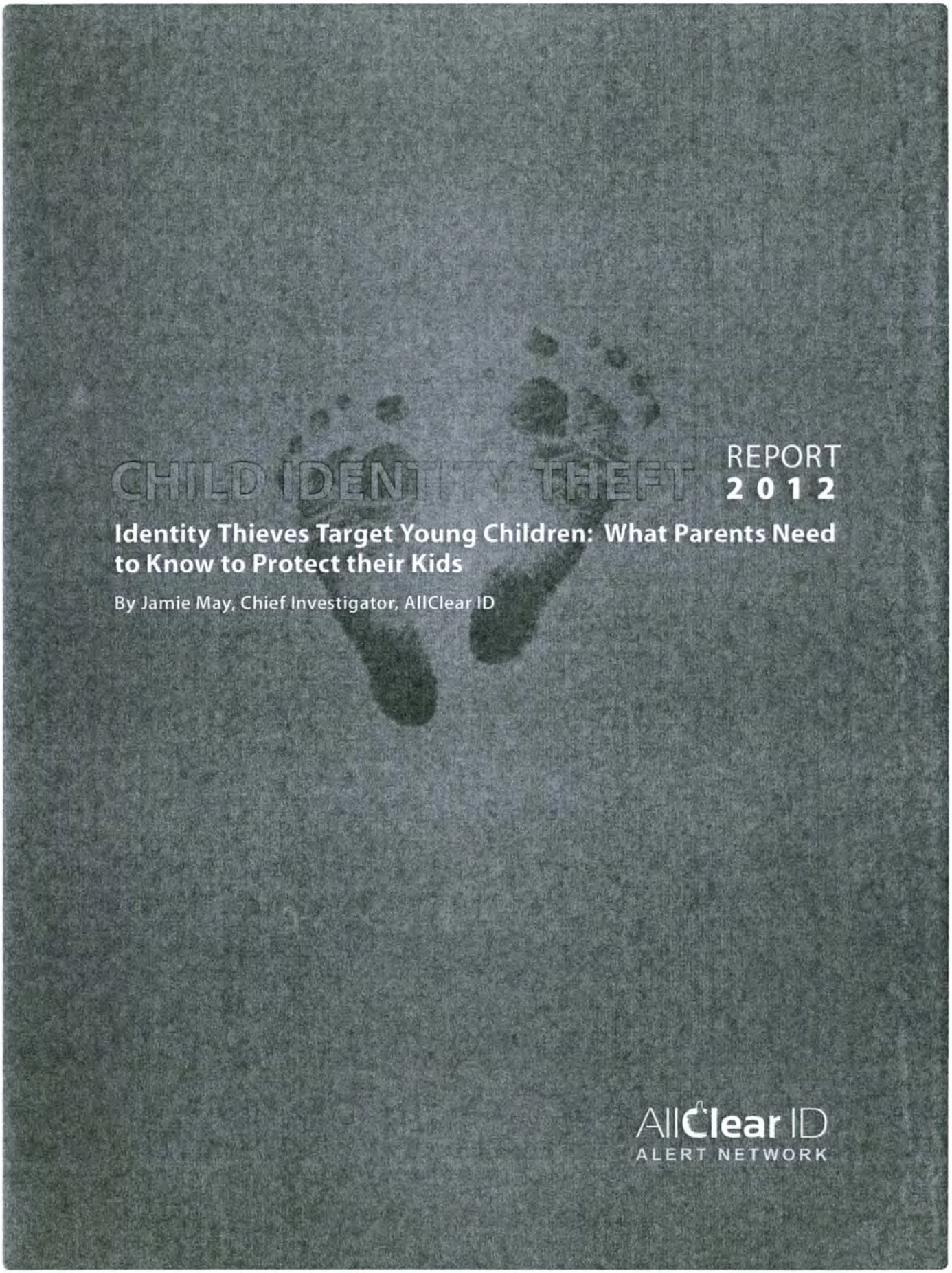
State	Citation	Who May Request a Freeze
Guam	None	
Hawaii	Hawaii Rev. Stat. §489P-1 *et seq.*	Any consumer who is a resident of the state
Idaho	Idaho Code §28-52-101 *et seq.*	Any consumer
Illinois	Ill. Rev. Stat. ch. 815, §505/2MM	Any consumer, including a representative on behalf of a disabled person appointed under Article XIa of the Probs of 1975 and under a written durable power of attorney that complies with the Illinois Power of Attorney Act or on b of a minor. The representative of a minor may be (1) a guardian of the minor that is the subject of the request, app under Article XI of the Probate Act of 1975; (2) a parent of the minor that is the subject of the request; and (3) a gu appointed under the Juvenile Court Act of 1987 for a minor under the age of 18 who is the subject of the request c a court order authorizing the guardian consent power, for a youth who is the subject of the request who has attain age of 16, but who is under the age of 21.
Indiana	Ind. Code §24-5-24-1 *et seq.* and Ind. Code §24-5-24.5-1 *et seq.*	Any consumer, including a representative of a "protected consumer," an individual who is: (1) less than 16 years or (2) an incapacitated person (as defined in IC 29-3-1-7.5) for whom a court has appointed a guardian.
Iowa	Iowa Code §714G.1 *et seq.*	Any consumer who is a resident of the state, including a representative of a "protected consumer," an individual v either under 16 years of age at the time a request for a protected consumer security freeze is made for the individ is an incapacitated person or a protected person for whom a guardian or conservator has been appointed.
Kansas	Kan. Stat. Ann. §50-701 *et seq.*	Any consumer
Kentucky	Ky. Rev. Stat. §367.363 *et seq.*	Any consumer
Louisiana	La. Rev. Stat. Ann. §9:3571.1	Any consumer, including a representative of a "protected consumer," an individual who is either of the following: (Under the age of 16 years at the time a request for the placement of a security freeze is made. (b) An interdicted p for whom a curator has been appointed, or an incapacitated person or a protected person for whom a guardian or conservator has been appointed.
Maine	Me. Rev. Stat. Ann. tit. 10, §1311 *et seq.* 2015 Chapter 139	A victim of identity theft or a consumer, including a representative of a protected consumer, who is an individual v has not attained 16 years of age at the time a request for the placement of a security freeze is made.
Maryland	Md. Commercial Code Ann. §1212.1 *et seq.*	Any consumer, including a representative of a "protected consumer," an individual who is: (i) Under the age of 16 at the time a request for the placement of a security freeze is made or (ii) An incapacitated person or a protected p for whom a guardian or conservator has been appointed in accordance with Title 13 of the Estates and Trusts Arti protected consumer includes an individual who: (i) Is in the custody of a local department; and (ii) Has been place foster care setting.
Massachusetts	Mass. Gen. Laws. Ann. ch. 93, §50 *et seq.*	Any consumer
Michigan	Mich. Comp. Laws §445.2511 *et seq.*	Any consumer, including a representative of a "protected consumer," (i) An individual who is under 16 years of ag the time a request for the placement of a security freeze is made. (ii) An incapacitated person or a protected perso whom a guardian or conservator has been appointed has been appointed under article V of the estates and protec individuals code, 1998 PA 386, MCL 700.5101 to 700.5520.
Minnesota	Minn. Stat. §13C.016 *et seq.*	Any consumer
Mississippi	Miss. Code Ann. §75-24-201 *et seq.*	Identity theft victim only
Missouri	Mo. Rev. Stat. §407.1380 *et seq.*	Any consumer

State	Citation	Who May Request a Freeze
Montana	Mont. Code Ann. §30-14-1726 *et seq.*	Any consumer, including a parent or guardian in the case of a minor or of an incapacitated person, or a conserva the case of a protected person.
Nebraska	Neb. Rev. Stat. §8-2601 *et seq.*	Any consumer, including a minor at the request of a parent or custodial parent or guardian if appointed.
Nevada	Nev. Rev. Stat. §598C.010 *et seq.*	Any consumer
New Hampshire	N.H. Rev. Stat. Ann. §359-B:22 *et seq.*	Any consumer
New Jersey	N.J. Rev. Stat. §56:11-30 *et seq.*	Any consumer
New Mexico	N.M. Stat. Ann. §56-3A-1 *et seq.*	Any consumer
New York	N.Y. General Business Law §380-a *et seq.* 2015 Chapter 3	Any consumer, including a protected consumer, who is an individual who is under the age of 16 years at the time request for the placement of a security freeze is made.
North Carolina	N.C. Gen. Stat. §75-60 *et seq.* 2015 Chapter 193	Any consumer, including a protected consumer who is an individual (i) who is under the age of 16 at the time a re for the placement of a security freeze is made pursuant to G.S. 75-63.1 or (ii) who is incapacitated or for whom a guardian or guardian ad litem has been appointed.
North Dakota	N.D. Cent. Code §51-33-01 *et seq.*	Any consumer
N. Mariana Islands	Statutes not available	
Ohio	Ohio Rev. Code Ann. §1349.52 *et seq.*	Any consumer
Oklahoma	Okla. Stat. tit. 24, §149	Any consumer
Oregon	Or. Rev. Stat. §646A.600 *et seq.*	Any consumer, including a representative of a "protected consumer," an individual who is: (a) Not older than 16 y old at the time a representative requests a security freeze on the individual's behalf; or (b) Incapacitated or for wh court or other authority has appointed a guardian or conservator.
Pennsylvania	Pa. Stat. tit. 73, §2501 *et seq.*	Any consumer
Puerto Rico	None	
Rhode Island	R.I. Gen. Laws §6-48-1 *et seq.*	Any consumer
South Carolina	S.C. Code Ann. §37-20-110 *et seq.*	Any consumer, including a representative of a "protected consumer," an individual who is: (a) under the age of 16 at the time a request for the placement of a security freeze is made; or (b) an incapacitated person or a protected for whom a guardian or conservator has been appointed.

State	Citation	Who May Request a Freeze
South Dakota	S.D. Codified Laws Ann. §54-15-1 *et seq.*	Identity theft victim only
Tennessee	Tenn. Code §47-18-2101 *et seq.* 2015 Public Chapter 282	Any consumer, including a representative of a protected consumer, who is (A) An individual who is under 16 year age at the time a request for the placement of a security freeze under this section is made; or (B) An incapacitatec person for whom a guardian or conservator has been appointed pursuant to title 34.
Texas	Tex. Business & Commerce Code Ann. §20.01 *et seq.* and Tex. Business & Commerce Code Ann. §20.21 *et seq.*	Any consumer, including a representative of a "protected consumer," an individual who resides in this state and is younger than 16 years of age at the time a request for the placement of a security freeze is made.
Utah	Utah Code Ann. §13-42-101 *et seq.* 2015 Chapter 191	A victim of identity theft or a consumer, including a representative of a protected consumer, who is an individual v the time a request for a security freeze is made, is: (a) less than 16 years of age; (b) an incapacitated person; or (protected person defined in §75-5b-102.
Vermont	Vt. Stat. Ann. tit. 9, §2480a *et seq.*	Any consumer
Virginia	Va. Code §59.1-444.1 *et seq.* 2014 Chapter 570	Any consumer who is a resident of the state, including a representative of a "protected consumer," a consumer w either: 1. Under the age of 16 years at the time a request for the placement of a security freeze is made; or 2. An incapacitated person for whom a guardian or conservator has been appointed in accordance with Chapter 20 (§64.2-2000 *et seq.*) of Title 64.2.
Virgin Islands	None	
Washington	Wash. Rev. Code §19.182.170 *et seq.*	Any consumer who is a resident of the state
West Virginia	W. Va. Code §46A-6L-101 *et seq.*	Any consumer
Wisconsin	Wis. Stat. §100.54 *et seq.*	A victim of identity theft or a consumer, including a representative of a "protected consumer," an individual who is the following: 1. Under the age of 16 years at the time a request for the placement of a security freeze is made un sub. (3)(a). 2. An individual for whom a guardian or conservator has been appointed.
Wyoming	Wyo. Stat. §40-12-501 *et seq.*	Any consumer

Total: 50 states and the District of Columbia

NCSL Contact: Heather Morton, Denver, (303) 364-7700


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.

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.

TABLE OF CONTENT

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

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.

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?

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 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*

AGE DISTRIBUTION:

Change from 2011 to 2012

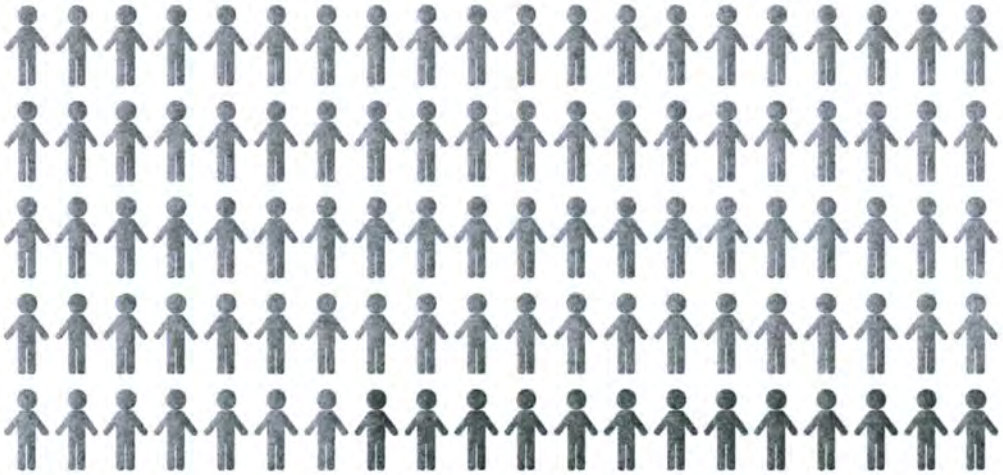
2,875 Possible Cases of Identity Theft

5 AND UNDER
426 Cases

AGE 6-10
759 Cases

AGE 11-14
843 Cases

AGE 15-18
848 Cases



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.*

.3%
Rate of **Adult** Attacks

10.7%
Rate of **Child** Attacks

Children are

35x

more likely to be victims than adults.

TYPES OF RECORDS INVOLVED IN CHILD IDENTITY THEFT CASES

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.*

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.

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.

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.

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.

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

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.

- **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.

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,

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

CHILD IDENTITY THEFT

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

By Richard Power,
Distinguished Fellow, Carnegie Mellon CyLab

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	2	3	4
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	Child IDs were used to purchase homes and automobiles, open credit card accounts, secure employment and obtain driver's licenses	The largest fraud ($725,000) was committed against a 16 year old girl	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?

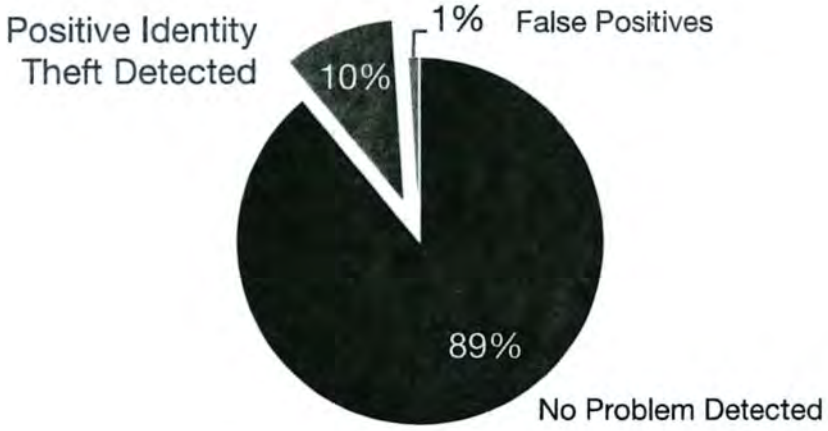
children had 51 times

higher attack rate than adults

GRAPHS & CHARTS

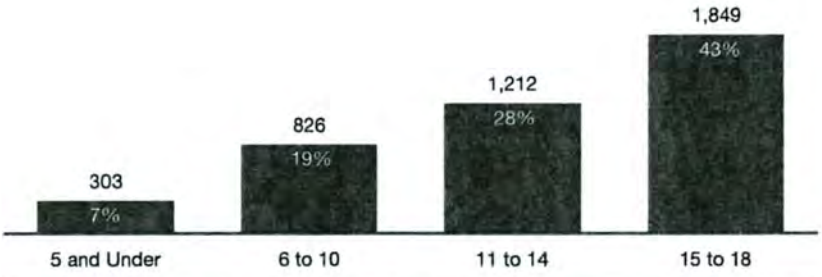
10.2% of Child Identities Scanned Exhibited Evidence of Identity Theft

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



Age Distribution: Possible Cases of Child Identity Theft

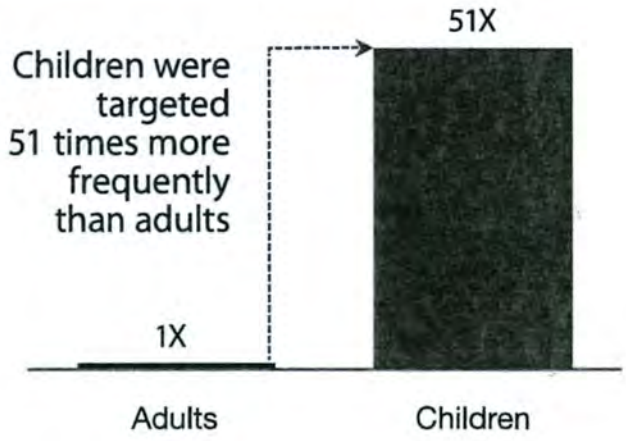
Total: 4,311 cases
Note: Age data not available on 121 children



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%)

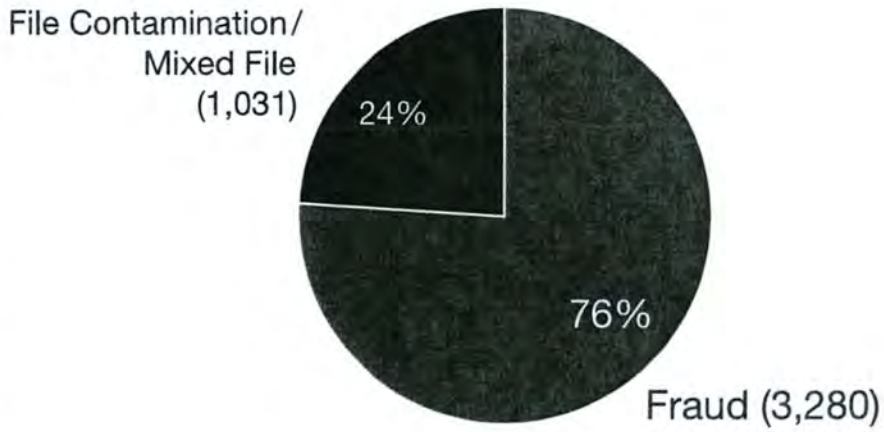
The chart to the right is based on 663 attacks against 347,362 adults and 4,311 attacks against 42,232 children, out of a total population of 351,673 (Source: Debix AllClear ID)



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.:

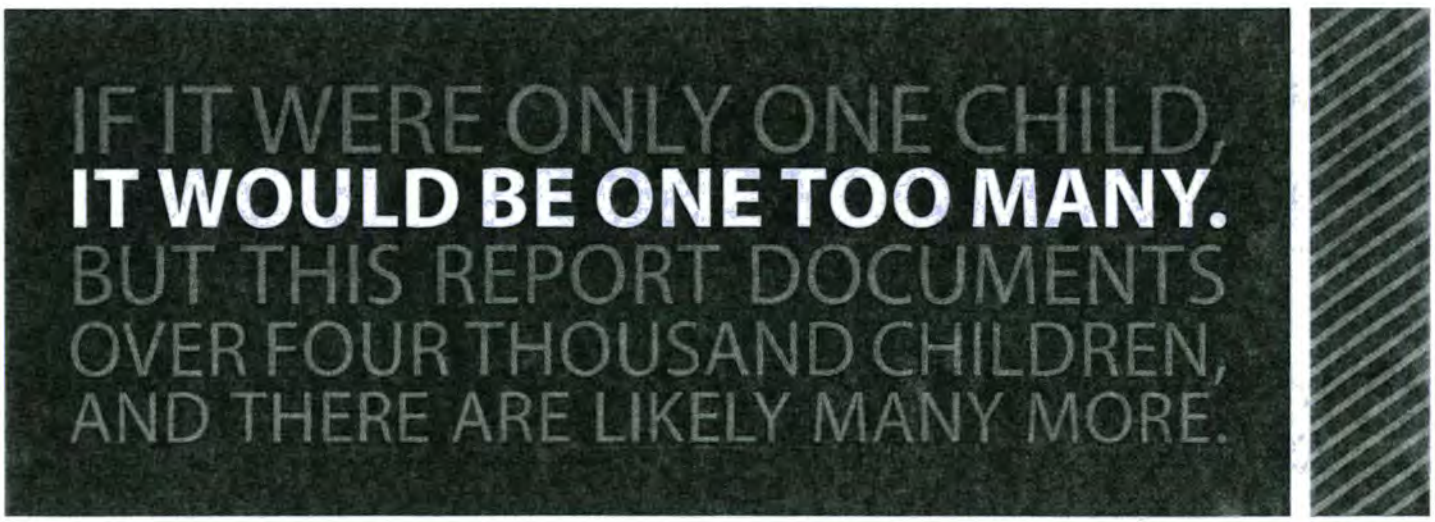
- *10.2% is a significant rate and is dramatically higher than the attack rate for adults. Parents need to think about their children's future, and take the time to look into this frequently overlooked problem*
- *Take steps to protect your children, especially in advance of key financial milestones 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.



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

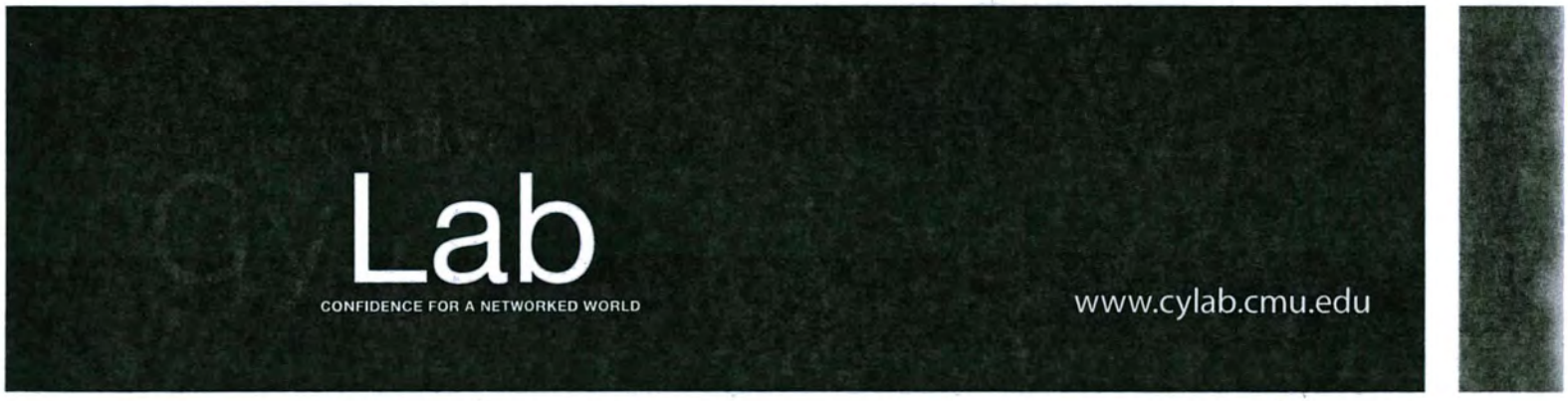
About AllClear ID

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


Lab
CONFIDENCE FOR A NETWORKED WORLD
www.cylab.cmu.edu

CDIA
CONSUMER DATA INDUSTRY ASSOCIATION
Empowering Economic Opportunity

April 13, 2016

The Honorable Gabrielle LeDoux
Chair, House Judiciary Committee
Juneau, Alaska

Re: Senate Bill 121 – Security Freeze for Minors

Dear Chairman LeDoux:

I write on behalf of the Consumer Data Industry Association (CDIA) to share our concerns related to Senate Bill 121, legislation seeking to create a mechanism to govern the placement, and removal of a security freeze for minors and protected consumers.

By way of background, CDIA was founded in 1906 and is the international trade association that represents some 120 consumer data companies. CDIA members represent the nation's leading institutions in credit reporting, fraud prevention, risk management, and employment reporting.

While CDIA is not opposed to purpose of Senate Bill 121, we are however, very concerned about the lack of consumer protections contained in the bill before your committee. The bill is limited in scope and does not contemplate a number of issues and situations which are critical to ensuring adequate protection of minor and otherwise vulnerable consumers. For example, the bill would require a consumer reporting agency to create a record and place it on a minor's file, however the term "record" is not defined in the bill, nor anywhere else in Alaska statue.

Additionally, by proposing that this new section be place in the adult security freeze portion of Alaska Code, it raises the likelihood that minors and other protected consumers will be subject to credit and identity fraud. Current Alaska Code allows for adults to easily place and remove security freezes within minutes. This makes sense for consumers who are active participants in the marketplace. However, for minors, this provision would open the door for unscrupulous actors to perpetrate fraud.

Finally, without proper authentication, consumers and their representatives will not be required to produce proof that they are who they say they are, or proof that they have legal authority to act on behalf of a minor or otherwise protected individual.

I hope this information has been helpful to you and your committee. Please feel free to reach out to me and CDIA throughout the legislative process, as we are happy to offer our subject matter expertise in this debate.

Respectfully submitted,

Ramon O. Looby
Senior Director, Public Policy & Government Relations

1090 Vermont Avenue, NW • Suite 200 • Washington, DC 20005 • Fax (202) 371-0134 •
www.cdiaonline.org

LEGAL SERVICES

DIVISION OF LEGAL AND RESEARCH SERVICES
LEGISLATIVE AFFAIRS AGENCY
STATE OF ALASKA

(907) 465-3867 or 465-2450
FAX (907) 465-2029
Mail Stop 3101

State Capitol
Juneau, Alaska 99801-1182
Deliveries to: 129 6th St., Rm. 329

MEMORANDUM April 14, 2016

SUBJECT: CSSB 121(JUD) relating to security freezes on the consumer credit report of a minor, incapacitated person, or protected person (Work Order No. 29-LS1129\E)

TO: Senator Kevin Meyer
Attn: Edra Morledge

FROM: Terry Bannister
Legislative Counsel

You have asked whether anything in the bill described above[1] or in current statute, specifically AS 45.48 (Personal Information Protection Act), precludes a credit reporting agency (agency) from establishing guidelines or policy for determining the authenticity of identification documents for a minor, protected person, incapacitated person, parent, legal guardian, or conservator.

The bill allows a parent, legal guardian, or conservator to make a request under the security freeze provisions of AS 45.48[2] for a minor, incapacitated person, or protected person. *The bill does not address identification requirements, but its reference to "under* AS 45.48.100 - 45.48.290" does require that an agency comply with the AS 45.48 security freeze requirements that apply to requests made under the bill.

The *AS 45.48* security freeze provisions are generally silent about identification, with certain limited exceptions. And there do not appear to be other provisions of AS 45.48 that apply to identification under the security freeze provisions.[3] With regard to the exceptions, the security freeze confirmation requirements of AS 45.48.120 require an agency to provide the requesting consumer with an identification device to use after the security freeze is in place. And the security freeze access provisions in AS 45.48.130 require the consumer to use the identification device and provide "proper identification to

---

[1] For the purposes of this memo, I am using CSSB 121(JUD) (Work Order No. 29-LS1129\E), which passed the Senate.

[2] AS 45.48.100 - 45.48.290.

[3] *See the exclusion from certain social security number request and collection* prohibitions under AS 45.48.410.

verify the consumer's identity" when allowing access during the security freeze. Any policy or guideline of an agency would have to comply with these requirements.

The security provisions appear to assume that an agency may develop policies and guidelines to implement the security freeze provisions. AS 45.48.130(j) refers to the "procedures used by a consumer credit reporting agency for implementing" AS 45.48.130. And, when a security freeze provision allows an agency to use telephone or electronic media, the provision adds "if the consumer credit reporting agency has developed procedures" for these approaches. These references to an agency's procedures suggest that the agency may establish guidelines and policies for establishing these procedures and that establishing policies and guidelines for identification is not inconsistent with the security freeze provisions.

I would conclude that the bill described above and AS 45.48, specifically the security freeze provisions, do not preclude a credit reporting agency from establishing identification guidelines or policy for identification where the security provisions of AS 45.48 are silent or need amplification, but that the guidelines and policy must be consistent with the security freeze provisions of AS 45.48.

If I may be of further assistance, please advise.

TLB:dla
16-472.dla