id:analytics®

WHITEPAPER

2011 Child Identity Fraud Study

July 2011

Table of Contents

Introduction

Traditional identity fraud protection services have limitations when it comes to protecting children from the impact of this insidious crime. These services typically rely on data contained within a credit report, which is a compilation of adult credit-related activity. Credit reports were never designed to effectively monitor a child's credit or identity behavior.

ID Analytics has taken an alternative approach to consumer identity protection with its Consumer Notification Service. The Consumer Notification Service does not rely on credit reports. It monitors use of consumers' identity information, such as name, address, date of birth and Social Security numbers (SSNs) and alerts consumers in real-time when their identity is used, potentially without their permission. If the consumer did not authorize the activity, the Consumer Notification Service provides consumers with a direct connection with the credit issuer to shut down the activity, often before it results in harm.

To provide greater insight into the scope of child identity fraud, ID Analytics conducted a study of more than 172,523 children enrolled in ID Analytics' Consumer Notification Service at some point during the 12-month period from April 1, 2010 to March 31, 2011. Seventy percent of the enrolled minors were 13 or under.

Key Findings

During the one-year period studied, ID Analytics found that:

- At least 142,000 identity frauds are perpetrated on children each year.
- Fifty five percent of the possible fraud cases identified by the Consumer Notification Service turned out to be legitimate fraud.
- Minors received proportionally 16 times fewer alerts than a comparable population of adults that received alerts during the same period.
- Conversely, minors who received an alert were seven times more likely to be victims of identity fraud than an adult. Minors received 0.5 percent of the identity use alerts. However, these yielded 3.5 percent of the cases of fraud.
- 60 percent of the identity alerts originated from the credit card industry. The vast majority of the remaining alerts were from the telecommunications industry, particularly wireless providers.

Background on Child Identity Fraud

Child identity fraud is a growing public concern. Children who have been victimized by identity fraud may face far reaching roadblocks as they enter adulthood and pursue employment and loans for higher education, cars or even purchasing their first home. Child identity fraud crimes can have deep roots, making it all that much harder to restore the victim's good name. Often, the crime can go undetected for years until a child reaches 18 and begins seeking credit.

Minors' identities are particularly appealing targets for fraudsters because their personal data is untainted, legitimate, less likely to be monitored for misuse, and few tools are available to protect children against attack.

Children's data is valuable: A minor's personal information has characteristics that make the data far more attractive to fraudsters than that of the general adult population. Minors, as a general rule, cannot legally apply for credit cards, so a thief knows a child's information is likely not associated with poor credit or linked to fraud. And the child has a legitimate SSN, which is a necessary precursor to many credit transactions. With a child's SSN, a fraudster can present a credit profile equivalent to that of an emerging or new consumer (immigrant, college graduate) who has not previously interacted with the credit environment.

Children's identities are more vulnerable: Children are soft targets to identity thieves. A thief knows that a child's identity information is less likely to be monitored than that of an adult.

Children are at particular risk of synthetic identity fraud, where a fraudster uses legitimate identity information to create a new, fake identity. A fraudster can misappropriate a child's SSN, and will have a better chance of success, because it will not trigger a match with another SSN in credit records that would likely result in further scrutiny. A common fraud scheme involves combining a child's legitimate SSN with other identity information to create an identity that passes traditional credit checks. Only years later, when affected children enter the credit market as adults, will they learn that their financial reputations are severely compromised.

Lack of effective tools to protect children's identities: As indicated above, children historically have had few available tools to protect them. Fraud prevention tools such as credit monitoring, free annual credit reports, and fraud alerts, all depend on the presence of a personal credit file. Children do not have credit files.

Research on Child Identity Fraud

What is the scope of the child identity fraud issue in the U.S.? Is it a raging pandemic or a more manageable problem? Recent research has given us better insight into the scope of these crimes against children.

1. Reports from the Federal Trade Commission Consumer Sentinel Database

Consumer Age	Complaints (%) 2007	Complaints (%) 2008	Complaints (%) 2009	Complaints (%) 2010
19 and under	19,800 (8%)	20,444 (7%)	19,196 (7%)	18,339 (8%)

Source: Federal Trade Commission (FTC), Consumer Sentinel Database

Child identity fraud complaints have consistently hovered around seven or eight percent of all FTC identity fraud complaints. According to the U.S. Census Bureau, in 2009, 24 percent of the U.S. population was under 18 and seven percent of the U.S. population was under the age of five.[i] Therefore, the proportion of child identity fraud claims in the Consumer Sentinel Database appears to be significantly lower than the proportionate representation of children in the general population.

The FTC statistics, while significant, most likely underestimate the relative prevalence of child identity fraud. How many pre-teen children would think to call the FTC fraud hotline on their own? One would expect that most of the callers are the victim's parents. Clearly, if a child's guardian or parent is committing the fraud, it won't be reported by the parent to the FTC. Additionally, even vigilant parents historically have had few tools to monitor their children's identity information for misuse. They simply are unaware that their child has been victimized.

2. ID Analytics 2011 ID Manipulation study

Earlier this year, ID Analytics conducted a first-of-its-kind study of individuals who deliberately manipulate identity information on applications for credit cards, cell phones, auto loans, and other credit transactions. Deliberate identity manipulation is defined as the **improper and intentional** alteration of key identity elements such as SSN, date of birth, and to a lesser degree—name, to obtain goods, services, or other benefits based on the misrepresentation of identity.

The study found that approximately two million American parents and children inappropriately share identity information. The study defined intergenerational identity sharing as two people using one last name, one SSN, different first names and two DOBs that differ by 18 to 25 years. This is an indication of parents and children sharing personally identifiable information.

The study did not attempt to determine whether a child stole his or her parent's identity or a parent misappropriated the child's identity, nor did the study restrict its view to parents of minors under 18. The data reflects both child and elder identity fraud. Nonetheless, this research does provide a reference point on the deliberate manipulation of children's identity by their parents. With more research, we can hone in on the actual proportion of intergenerational identity fraud conducted by children and the proportion conducted by parents.

3. Study of Child Identity Use and Misuse

ID Analytics' study examined the use and misuse of more than 172,523 children's identities that were enrolled in its ID Analytics Consumer Notification Service at some point during the 12-month period, from April 1, 2010 to March 31, 2011. Seventy percent of the minors were under 13.

Description of Consumer Notification Service (CNS)

Consumer Notification Service is ID Analytics' identity monitoring and alerting service which powers the majority of the nation's leading identity monitoring services. ID Analytics' service does not rely on credit bureau data. Instead, ID Analytics Consumer Notification Service monitors for use of consumers' identity information, such as name, address, date of birth and Social Security numbers (SSNs) and alerts consumers in real-time when their identity is used, potentially without their permission.

Through the Consumer Notification Service, individuals have real time insight into the use of their personal identity information. The service links millions of consumers with the nation's leading credit card companies, banks, wireless providers, auto lenders, retailer card issuers, check issuers, and utilities.

If the identity use is deemed inappropriate, the consumer simply responds to the alert—"that's not me." In this way, they can use ID Analytics' patent-pending Not Me™ Notification System to stop the fraudulent activity. This service is available to children as well. In the case of a child, the child's parent or guardian enrolls the child and receives the alerts on the child's behalf.

Consumers (typically parents) provide ID Analytics with their child's personal information. ID Analytics checks incoming applications for credit and services, account address change requests, and other identity events in the ID Network® for use of the child's SSN and for combinations of the child's name, date of birth, address, and phone. The service alerts on any activity detected in the ID Network.

The ID Network has over 1.4 billion identity events from applications for products and services where identity information is required. The network operates in real time and receives millions of transactions a month from leading companies. Since children are generally prohibited from applying for credit, most instances of their identity information within the ID Network are likely indicative of either an error or fraud.

Because of ID Analytics' long standing work in protecting both organizations and consumers from identity fraud, the company has direct connections to the fraud departments of leading companies. When a consumer alerts ID Analytics of a potential fraud using the Not Me Notification System, ID Analytics works with the credit issuer to shut it down.

ID Analytics Research Findings

The following table describes the alerts and cases linked to children from the Consumer Notification Service during the period of April 1, 2010 to March 31, 2011. Alerts refer to messages sent to consumers by ID Analytics' Consumer Notification Service indicating that their personal information (SSN and date of birth) was used in credit activity. Cases are a subset of alerts that consumers, in conjunction with ID Analytics' customer care office, determined were potentially fraudulent and merited further investigation by the credit issuer.

	Minors Age 0-13	Minors Age 14 through 17
Alerts	1,787	742
Cases	415	186
Confirmed Frauds	228	102

During the study period, children received 2,529 alerts. Minors age 14 through 17 received 742 alerts and minors under 13 received 1,787 alerts. It is worth noting that the study reflects the cumulative enrolled population during the study period, and not all children received alerts for the 12-month period. Some children began their enrollment after the April 1, 2010, while others had their commercial service cancelled during the period.

Most of the alerts came from either credit or cell phone applications. Sixty percent of the Consumer Notification Service alerts to minors came from the credit industry, 31 percent wireless or landline phone industry, and five percent of the alerts came from auto loans.

The consumer and the Consumer Notification Service collaboratively identified 601 cases of possible fraud which were referred to credit issuers for further review. Of the 601 cases of possible fraud referred to credit issuers, the organizations determined that 330 cases were true fraud. In total, 55 percent of the potential fraud cases turned out to be fraud.

In sum, less than one percent (300 out of 172, 000) of the children enrolled in the Consumer Notification Service experienced identity fraud. This percentage is likely an underestimate of the overall rate of identity fraud experienced by children for several reasons. First, the study sample included minors who either enrolled or dropped out of the service after April 1, 2010. Second, enrollees in identity monitoring services reflect a biased sample. A parent who enrolls his or her child in an identity monitoring service is unlikely to be stealing that child's information. Finally, ID Analytics' monitoring service, like any service, does not provide a universal source of child data use. The service focuses on credit applications, auto loans, phone applications, utility applications, checking accounts, and account address request changes. It does not include information on identity fraud related to employment, government benefits, or medical claims.

Comparisons to Incidences of Adult Population Identity Fraud

The study then compared alerts and cases involving minors to a comparable adult population for the same period. In general, we found that minors received fewer alerts, but a higher proportion of the alerts proved to be fraudulent transactions.

Specifically, minors received proportionally 16 times fewer alerts than a comparable population of adults getting alerts during the same period. A minor who did receive an alert was seven times more likely to be a victim of fraud than an adult. Minors received 0.5 percent of the alerts. However, these alerts yielded 3.5 percent of the cases of fraud.

These findings are consistent with general operational rules of the credit reporting system. As a general rule, children's identifying information such as their SSN, name and date of birth should not appear in applications for credit cards, retail cards, cell phones or other credit activity. If the child's information does appear, it is likely to be fraud, which we found to be true in 55 percent of the cases.

Conclusion

This paper discusses the application of ID Analytics Consumer Notification Service to child identity fraud. The Consumer Notification Service fills an historical gap in child identity fraud protection by allowing children, just like adults, to have the use of their identity information monitored for use or misuse. Through its Consumer Notification Service, ID Analytics monitors real-time transactions throughout the U.S. for use and misuse of a child's SSN, name, date of birth, and other information. While adults have historically had access to credit monitoring services built on credit files, the Consumer Notification Service connects children's parents and guardians directly with credit issuers to monitor in real time the use of their child's personal information, and provides a mechanism to block fraudulent transactions.

In this study, ID Analytics Consumer Notification Service stopped over 300 cases of fraud. These cases of fraud represent real financial losses. Each instance of fraud stopped saves $3,000 for the card issuer, $300 for wireless, and $1,000 for cable/satellite service providers.

The Consumer Notification Service is an example of the technologies that have emerged in the marketplace to combat child identity fraud. As with other aspects of the identity fraud problem, there is no silver bullet remedy. Child identity fraud poses complex challenges to consumers, businesses, and regulators. A comprehensive solution to child identity fraud requires a layered approach reflecting advances in technology and business processes, legislative guidance and consumer education.

[i] http://quickfacts.census.gov/qfd/states/00000.html

id:analytics®

www.idanalytics.com