

**BEFORE THE SOCIAL SECURITY ADMINISTRATION**

**In the Matter of Request for Comment on Assigning New Social Security Numbers for  
Children Age 13 and Under**

**Docket No. SSA 2012-0042**

**Comments of the Staff of the Federal Trade Commission  
Bureau of Consumer Protection\***

**April 11, 2013**

---

**\* These comments represent the views of the staff of the Bureau of Consumer Protection. They are not necessarily the views of the Commission or any individual Commissioner.**

## I. Introduction

On February 11, 2013, the Social Security Administration (SSA) issued a request for comment on its proposed policy change for assigning new Social Security Numbers (SSNs) to children age 13 and under in certain circumstances. SSA proposes to assign new SSNs when the child's Social Security card has been stolen in transit; the child's SSN has been incorrectly disclosed through SSA's publicly available Death Master File; or when a third party has misused the child's SSN. Specifically, the request for comment asked three questions: (1) whether age 13 is the appropriate cut-off for application of the revised policy; (2) whether the proposed circumstances for assigning a new SSN are appropriate; and (3) whether there are other circumstances that would warrant assignment of a new SSN to children age 13 and under.

Federal Trade Commission (FTC or Commission) staff supports the SSA's proposal to revise its policy for assigning new SSNs for children in some circumstances. Based on its own research, education and outreach experience, FTC staff believes that the proposed changes will help many children, parents, and guardians address the harms stemming from misuse of children's SSNs.

## II. FTC Efforts to Mitigate Identity Theft

The FTC has a vigorous law enforcement program to protect consumers' privacy, as well as a strong outreach program to educate consumers on identity theft.<sup>1</sup> Millions of consumers are victimized by identity thieves each year,<sup>2</sup> collectively costing consumers and businesses billions of dollars<sup>3</sup> and countless hours to repair the damage. SSNs are particularly valuable to identity thieves in committing many types of identity theft. Criminals obtain the SSNs of victims through many different schemes, and then fraudulently use the SSNs to open new accounts, gain access to existing accounts, commit medical identity theft, seek employment, and obtain government benefits.<sup>4</sup> The FTC has worked to combat identity theft and mitigate its effects in a number of ways:

- The Commission works to empower consumers by providing them with the knowledge and tools to protect themselves from identity theft and to deal with the consequences when it does occur. For example, the FTC publishes a victim recovery guide, *Taking Charge*, that explains the immediate and long-term steps identity theft victims should take to address the crime.<sup>5</sup> Other materials explain

---

<sup>1</sup> See Identity Theft and Assumption Deterrence Act, Pub. L. 105-318, 112 Stat. 3007 (1998). Among other things, this Act directs the FTC to establish the federal government's central repository for identity theft complaints and to provide victim assistance and consumer education.

<sup>2</sup> See Bureau of Justice Statistics, *National Crime Victimization Survey Supplement, Victims of Identity Theft*, 2008 (Dec. 2010) at 1-2 (finding 11.7 million persons, representing 5% of all Americans age 16 or older, were victims of identity theft during a two-year period).

<sup>3</sup> *Id.* at 4 (finding the total financial cost of identity theft was \$17.3 billion over a two-year period).

<sup>4</sup> See *Protecting Social Security Numbers from Identity Theft: Hearing Before the Subcommittee on Social Security of the House Committee on Ways and Means, United States House of Representatives*, 112th Cong. (2011), available at <http://www.ftc.gov/os/testimony/110411ssn-idtheft.pdf>.

<sup>5</sup> Available at [www.ftc.gov/bcp/ed/pubs/consumers/idtheft/idt04.pdf](http://www.ftc.gov/bcp/ed/pubs/consumers/idtheft/idt04.pdf).

how to obtain a free credit report and correct fraudulent information in credit reports; how to file a police report, and how to protect personal information.<sup>6</sup>

- In 2008, the Commission issued a report on preventing the misuse of SSNs in the private sector.<sup>7</sup> Private and public sector entities have used the SSN extensively as an identifier and in the authentication process for employment, insurance, credit and housing. As a result, the SSN has become both more available and more valuable to identity thieves. The report recommended that Congress consider taking action to strengthen the procedures that private-sector organizations use to authenticate their customers' identities, and that steps be taken to reduce the unnecessary display and transmission of SSNs.
- The Commission encourages companies to secure consumers' personal information so that it does not fall into the hands of identity thieves. Since 2001, the Commission has brought forty-two law enforcement actions against businesses that failed to reasonably protect sensitive consumer information that they maintained. One of the best-known FTC cases from our data security program is the 2006 action against ChoicePoint, Inc., a data broker that sold more than 160,000 consumers' sensitive information, including SSNs, to data thieves posing as ChoicePoint clients.<sup>8</sup> The thieves used that information to steal the consumers' identities.<sup>9</sup>
- In carrying out the Commission's identity theft consumer outreach mission, FTC staff often examines how to target its efforts toward populations especially vulnerable to the crime, such as children. To this end, in 2011, the FTC co-hosted a forum on child identity theft. Panelists discussed how, through a variety of means, identity thieves deliberately capture and use the SSNs of children, or fabricate SSNs that coincidentally have been assigned to children, in order to obtain employment, government benefits, or credit.<sup>10</sup> Since our forum, we have conducted outreach to schools and to parents, partnered with other organizations

---

<sup>6</sup> Available at <http://www.consumer.ftc.gov/features/feature-0014-identity-theft>.

<sup>7</sup> FTC, *Security in Numbers, SSNs and ID Theft* (Dec. 2008), available at [www.ftc.gov/os/2008/12/P075414ssnreport.pdf](http://www.ftc.gov/os/2008/12/P075414ssnreport.pdf).

<sup>8</sup> *United States v. ChoicePoint, Inc.*, No. 106-CV-0198 (N.D. Ga.) (settlement entered on Feb. 15, 2006). More recent data security cases involving SSNs include *In the Matter of CBR Systems, Inc.*, F.T.C. File No. 112 3120 (2013) (pending final Commission approval); *U.S. v PLS Financial Services, Inc.*, No. 1:12-CV-08334 (N.D. Ill. 2012); and *In re Ceridian Corporation*, F.T.C. Dkt. No. C-4325 (2011).

<sup>9</sup> In settling the case, ChoicePoint agreed to pay \$10 million in civil penalties for violations of the FCRA and \$5 million in consumer redress for identity theft victims, and agreed to undertake new data security measures. See *ChoicePoint, Inc.*, No. 106-CV-0198 (N.D. Ga.) (settlement entered on Feb. 15, 2006).

<sup>10</sup> See *Stolen Futures: A Forum on Child Identity Theft* ("Stolen Futures"), [www.ftc.gov/bcp/workshops/stolenfutures](http://www.ftc.gov/bcp/workshops/stolenfutures) (also containing a link to a webcast and transcripts of the Forum); see also Press Release, *FTC, Department of Justice to Host Forum on Child Identity Theft* (June 2, 2011), available at [www.ftc.gov/opa/2011/06/childtheft.htm](http://www.ftc.gov/opa/2011/06/childtheft.htm).

to conduct outreach, testified before Congress<sup>11</sup> and monitored developments in this area, as described below.

### III. Child Identity Theft

Recent studies have explored the prevalence of child identity theft. One 2011 study estimated that 142,000 instances of identity fraud are perpetrated on minors in the United States each year.<sup>12</sup> Another study surveyed 40,000 children who had been enrolled in an identity protection service. It found that 4,311 of those children (10.2%) had loans, property, utility, and other accounts associated with their SSNs.<sup>13</sup>

A more recent 2012 study found that 2.5% of U.S. households with minor children suffer child identity theft during the child's life, and the theft or misuse of SSNs is the most common way a child's information is exploited.<sup>14</sup> Children's names, addresses, dates of birth, and health information can also be misused. Child identity theft is especially pernicious because the theft may not be detected until the child is older and seeks employment, or applies for student or car loans.

The Commission co-hosted its forum on child identity theft to gain a greater understanding of the distinct challenges these victims face.<sup>15</sup> The forum highlighted the fact that a child's unused SSN is uniquely valuable to identity thieves because it typically lacks a previous credit history and can be paired with any name and birth date.<sup>16</sup> In the eyes of thieves, a child's identity is unblemished and can be exploited over a long period of time, especially because parents generally do not monitor their children's credit files for misuse, as children typically do not have credit files.

---

<sup>11</sup> See *Child Identity Theft: Field Hearing Before the Subcommittee on Social Security of the Committee on Ways and Means, United States House of Representatives*, 112th Cong. (2011), available at <http://www.ftc.gov/os/2011/09/110901identitythefttestimony.pdf>.

<sup>12</sup> See ID Analytics, *More Than 140,000 Children Could Be Victims of Identity Fraud Each Year* (July 12, 2011), available at [www.idanalytics.com/news-and-events/news-releases/2011/7-12-2011.php](http://www.idanalytics.com/news-and-events/news-releases/2011/7-12-2011.php). ID Analytics, which offers credit monitoring services, noted that this figure is under-representative of the actual rate of child identity theft because the sample was self-selected, focusing on children enrolled in their credit monitoring service, and likely does not include instances of parents who may victimize their own children. Nor does the study reach all uses of child data for fraud (e.g., identity theft involving medical claims, government benefits, and employment, which typically do not appear in a credit report).

<sup>13</sup> See Richard Powers, Carnegie Mellon CyLab, *Child Identity Theft: New Evidence Indicates Identity Thieves are Targeting Children for Unused Social Security Numbers* (2011), available at [www.cylab.cmu.edu/files/pdfs/reports/2011/child-identity-theft.pdf](http://www.cylab.cmu.edu/files/pdfs/reports/2011/child-identity-theft.pdf).

<sup>14</sup> See Identity Theft Resource Center, *ITAC Announces Results of Child Identity Fraud Survey Report*, (December 4, 2012), available at [http://identitytheftassistance.org/uploaded\\_files/fck/ITAC\\_child\\_ID\\_theft\\_PR\\_12\\_4\\_2012.pdf](http://identitytheftassistance.org/uploaded_files/fck/ITAC_child_ID_theft_PR_12_4_2012.pdf).

<sup>15</sup> See *Stolen Futures*, *supra* note 10.

<sup>16</sup> Following the forum, the Commission published a comprehensive guide for parents on child identity theft: *Safeguarding Your Child's Future*, available at <http://www.consumer.ftc.gov/articles/pdf-0010-child-identity-theft.pdf>.

#### IV. Comments Regarding Proposed Policy Change

The FTC staff supports the SSA in its efforts to revise its policy for assigning new SSNs for children age 13 and under. Staff believes SSA's proposed new policy promises to be a helpful tool for children and their parents and guardians, as they work to undo the harms resulting from misuse of the child's SSN. As discussed above, studies and outreach efforts have revealed child identity theft to be a serious issue that has wide-ranging and severe consequences. The repercussions can be severe because some legal tools available to aid adults are not helpful to children. For example, a fraud alert, which a consumer can activate to warn potential creditors of possible identity theft, is premised on the existence of that consumer's credit file. Because children typically do not have credit files before becoming victims of identity theft, parents cannot use fraud alerts to proactively protect their children. In addition, children may not take advantage of other remedies, which typically require a victim to obtain a police report to document the crime.<sup>17</sup> Children victimized by parents or guardians are often reluctant to file a police report naming a family member or friend as the perpetrator once they discover the identity theft.<sup>18</sup>

The opportunity to receive a new SSN where there has been apparent misuse would give many more victimized children the chance to begin adulthood with the unblemished credit history and financial reputation they deserve. In particular, we support SSA's proposal to no longer require proof that the child was harmed due to the misuse of his or her SSN when there is evidence that the SSN is being misused (e.g., for employment purposes or as identification to a police officer). Indeed, even in instances of identity theft relating to financial fraud, it can be difficult to demonstrate that the harm is traceable to the misuse of the SSN as opposed to misuse of some other credential.

The FTC offers the following comments on questions one and two posed in the notice.

1. *Is age 13 the appropriate cut-off for application of the revised policy?*

FTC staff respectfully proposes that the SSA raise the cut-off age for this policy change. Misuse of SSNs can happen to teenagers age 14 to 17, and the repercussions are just as severe as when it occurs to a younger child. Indeed, even when the misuse of an SSN occurs before age 14, the harm is often undiscovered until age 16 or older, when the minor seeks credit, an apartment, or a job. As currently drafted, the revised policy will not aid all victimized children.

The limitations of the SSA proposal are especially relevant to children in foster care. Children in foster care are particularly vulnerable to identity theft due to the wide circulation of their personal information. To assist these children, the Child and Family Services Improvement and Innovation Act, signed into law in September 2011, directs state child welfare agencies to

---

<sup>17</sup> These remedies include extended fraud alerts, access to documents underlying the theft, and blocking of erroneous debts.

<sup>18</sup> See generally Transcript of Stolen Futures, Session 2, Remarks of Linda Foley, Russell Butler, and Theresa Ronnebaum, available at [http://htc-01.media.globix.net/COMP008760MOD1/ftc\\_web/FTCindex.html#July12](http://htc-01.media.globix.net/COMP008760MOD1/ftc_web/FTCindex.html#July12).

provide a credit report to each child who reaches age 16 while in the state's foster care. The Act also directs the child welfare agencies to assist in interpreting the report, and resolving any inaccuracies it contains.<sup>19</sup> Expanding the SSA's proposal to include children under 18 years old would assist child welfare agencies by creating another tool with which to address the harms resulting from the misuse of foster children's SSNs.

2. *Are the circumstances that we propose for assigning a new SSN to children age 13 and under appropriate?*

Commission staff endorses the three circumstances under which the SSA would be willing to provide a new SSN, with one revision to refine the third circumstance. As currently drafted, a new SSN would be assigned when "[a] third party misused the child's SSN." 78 Fed. Reg. at 9766. This criterion is vague as to who may alert the SSA of the misuse. We support a revision that would make clear that law enforcement agencies and child welfare agencies could alert the SSA of misuse by including new language, such as: "a third party has misused the child's SSN, based on information from a parent, a guardian, a law enforcement agency or a child welfare agency." It is important to clarify this point because many instances of child identity theft involve individuals who are family, or closely associated with the child. In these instances, the individual would be unlikely to report the misuse to the SSA, whereas law enforcement agencies are investigating the issue of identity theft generally, and could report misuse of SSNs to the SSA as they become aware of it.

## V. Conclusion

The Commission supports SSA's effort to revise the policy on assigning new SSNs to children age 13 and under, as it will help children recover from the negative consequences of identity theft. FTC staff hopes its recommendations prove useful to SSA and appreciates its consideration of them. If you have any questions about this comment or would like additional information, please contact Maneesha Mithal, Associate Director, Division of Privacy and Identity Protection, at (202) 326-2771.

Respectfully submitted,

---

Charles A. Harwood, Acting Director  
Maneesha Mithal, Associate Director  
Mark Eichorn, Assistant Director  
Lisa Schifferle, Attorney  
Steven Toporoff, Attorney  
Megan Cox, Attorney  
Bureau of Consumer Protection

---

<sup>19</sup> The Child and Family Services Improvement and Innovation Act, 42 U.S.C. § 675 (2011). Available at <http://www.govtrack.us/congress/bills/112/hr2883/text>.