PREPARED STATEMENT OF
THE FEDERAL TRADE COMMISSION

Before the

SUBCOMMITTEE ON SOCIAL SECURITY

of the

HOUSE COMMITTEE ON WAYS AND MEANS

on

Child Identity Theft

Field Hearing
Plano, Texas

September 1, 2011

I. INTRODUCTION

Chairman Johnson, Ranking Member Becerra, and Members of the Subcommittee, I am Deanya Kueckelhan, Director of the Southwest Regional Office of the Federal Trade Commission ("FTC" or "Commission").[1] I appreciate the opportunity to present the Commission's views on child identity theft. Protecting consumers especially vulnerable consumers such as children against identity theft and its consequences is a critical component of the Commission's consumer protection mission.[2]

This testimony begins by describing the nature of identity theft generally and the Commission's law enforcement, nationwide complaint management, and education and outreach efforts on identity theft. In particular, it describes some of the 34 actions the Commission has brought since 2001 against businesses that allegedly failed to reasonably protect sensitive consumer information that they maintained. It then describes *Stolen Futures*, a recent forum on child identity theft held on July 12, 2011, co-sponsored by the FTC and the Department of Justice's Office for Victims of Crime. Finally, the testimony discusses next steps to combat this problem.

---

[1] The views expressed in this statement represent the views of the Commission. My oral presentation and responses to questions are my own and do not necessarily represent the views of the Commission or any individual Commissioner.

[2] *See* Identity Theft and Assumption Deterrence Act, Pub. L. 105-318, 112 Stat. 3007 (1998). Criminal prosecutions under the Act are handled by the United States Department of Justice. The Act directs the FTC, a civil law enforcement agency, to establish the federal government's central repository for identity theft complaints and to provide victim assistance and consumer education. The repository of identity theft complaints, known as the "Identity Theft Clearinghouse," is discussed in greater detail below in Section II.

II. IDENTITY THEFT

Millions of consumers are victimized by identity thieves each year,[3] collectively costing consumers and businesses billions of dollars[4] and countless hours to repair the damage. Given the serious and widespread harm caused by identity theft, the Commission has devoted significant resources toward combating the problem, acting aggressively on three main fronts: law enforcement, nationwide complaint management, and education.

A. Law Enforcement

The Commission enforces a variety of laws requiring entities, in certain circumstances, to have reasonable procedures in place to secure consumer information so that it does not fall into the hands of identity thieves or other unauthorized persons. For example, the Commission's Safeguards Rule under the Gramm-Leach-Bliley Act establishes data security requirements for financial institutions.[5] The Fair Credit Reporting Act ("FCRA") requires consumer reporting agencies to use reasonable procedures to ensure that the entities to which they disclose consumer reports have a permissible purpose for receiving that information,[6] and imposes safe disposal

---

[3] *See* Bureau of Justice Statistics, *National Crime Victimization Survey Supplement, Victims of Identity Theft, 2008* (Dec. 2010) ("BJS Supplement") 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 ending in 2008).

[4] *Id.* at 4 (finding the total financial cost of identity theft was 17.3 billion dollars during a two-year period ending in 2008).

[5] 16 CFR Part 314, implementing 15 U.S.C. § 6801(b). The Federal Deposit Insurance Corporation, National Credit Union Administration, Securities and Exchange Commission, Office of the Comptroller of the Currency, Board of Governors of the Federal Reserve System, Office of Thrift Supervision, Secretary of the Treasury, and state insurance authorities have promulgated comparable safeguards requirements for the entities they regulate.

[6] 15 U.S.C. § 1681e.

obligations on entities that maintain consumer report information.[7] In addition, the Commission enforces the FTC Act's proscription against unfair or deceptive acts or practices[8] in cases where a business makes false or misleading claims about its data security procedures, or where its failure to employ reasonable security measures causes or is likely to cause substantial consumer injury that is not reasonably avoidable by consumers and not outweighed by countervailing benefits.

Since 2001, the Commission has brought 34 law enforcement actions against businesses that allegedly failed to reasonably protect sensitive consumer information that they maintained. One of the best-known FTC data security cases is the 2006 action against ChoicePoint, Inc., a data broker that allegedly sold sensitive information (including Social Security numbers ("SSNs") in some instances) concerning more than 160,000 consumers to data thieves posing as ChoicePoint clients.[9] In many instances, the thieves used that information to steal the consumers' identities. The Commission alleged that ChoicePoint failed to use reasonable procedures to screen prospective purchasers of the consumers' information and ignored obvious security red flags. For example, the FTC alleged that the company approved as purchasers individuals who lied about their credentials, used commercial mail drops as business addresses, and faxed multiple applications from public commercial photocopying facilities. In settling the

---

[7] *Id.* at § 1681w. The FTC's implementing rule is at 16 CFR Part 682.

[8] 15 U.S.C. § 45(a).

[9] *United States v. ChoicePoint, Inc.,* No. 106-CV-0198 (N.D. Ga.) (settlement entered on Feb. 15, 2006).

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.[10]

Most recently, in June of this year, the Commission resolved allegations that Ceridian Corporation[11] and Lookout Services, Inc.,[12] violated the FTC Act by failing to implement reasonable safeguards to protect the sensitive consumer information they maintained. The companies offered, respectively, payroll processing and immigration compliance services for small business employers. As a result, they both obtained, processed, and stored highly-sensitive information including SSNs of employees. The Commission alleged that both companies failed to appropriately safeguard this information, which resulted in intruders being able to access it. The orders require the companies to implement comprehensive data security programs and obtain independent audits for 20 years.

B. Nationwide Complaint Management and Analysis

In addition to law enforcement, the Commission collects, manages, and analyzes identity theft complaints in order to target its education efforts and assist criminal law enforcement authorities. The Commission manages the Identity Theft Clearinghouse, a secure online

---

[10] In 2009, the Commission charged that the company violated the earlier court order and obtained a stipulated modified order under which ChoicePoint agreed to expand its data security obligations and pay monetary relief in the amount of $275,000. *United States v. ChoicePoint, Inc.*, No. 1:06-CV-0198-JTC (N.D. Ga. 2009) (settlement entered on Oct. 14, 2009).

[11] *Ceridian Corp.*, FTC Docket No. C-4325 (June 8, 2011) (consent order), *available at* www.ftc.gov/opa/2011/05/ceridianlookout.shtm.

[12] *Lookout Servs., Inc.*, FTC Docket No. C-4326 (June 15, 2011) (consent order), *available at* www.ftc.gov/opa/2011/05/ceridianlookout.shtm.

database of identity theft-related complaints. Identity theft victims can enter complaint information directly into the database via an online complaint form or by calling a toll-free identity theft hotline and speaking with a trained counselor. The Commission makes the Clearinghouse data available to over 2,000 American and Canadian federal, state, and local law enforcement agencies who have signed confidentiality and data security agreements.[13] Through the Clearinghouse, law enforcers can search identity theft complaints submitted by victims, law enforcement organizations, and the Identity Theft Assistance Center, a not-for-profit coalition of financial services companies. To assist law enforcement and policy makers, the FTC also routinely issues reports on the number and nature of identity theft complaints received by the FTC.[14]

C. Consumer, Business, and Other Education

Consumer education and outreach is another important part of the Commission's mission. 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. The Commission receives on average 35,000 consumer contacts each week through its toll-free hotline and dedicated website, of which approximately 5,600 are identity theft

---

[13] For example, each of the 50 Offices of the Attorney General has access to the Clearinghouse data.

[14] *See*, *e.g.*, FTC, *Consumer Sentinel Network Data Book for January - December, 2010* (Feb. 2011), *available at* http://ftc.gov/sentinel/reports/sentinel-annual-reports/sentinel-cy2010.pdf. The 2010 Data Book shows that over 250,000 consumers reported some form of identity theft, which represents 19% of the total number of complaints submitted to the Commission. This makes identity theft the most frequently reported category of consumer complaints, continuing a pattern that started over a decade ago. The Data Book also shows that Texas ranks fifth among the states in identity theft complaints after Florida, Arizona, California, and Georgia, with 24,158 complaints submitted to the Commission (96.1 complaints per 100,000 population) during the time period measured.

complaints. Callers to the hotline receive counseling from trained personnel on steps they can take to prevent or recover from identity theft.

Further, the FTC makes available a wide variety of consumer educational materials, including many in Spanish, to help consumers deter, detect, and defend against identity theft. For example, the FTC publishes a victim recovery guide *Take Charge: Fighting Back Against Identity Theft*[15] that explains the immediate steps identity theft victims should take to address the crime; how to obtain a free credit report and correct fraudulent information in credit reports; how to file a police report;[16] and how to protect their personal information. The Commission has distributed over 3.8 million copies of the recovery guide and has recorded over 3.5 million visits to the Web version.

The Commission also sponsors a multimedia website, OnGuard Online,[17] designed to educate consumers about basic computer security, including the importance of not disclosing personal information such as SSNs to possible fraudulent operators. OnGuard Online was developed in partnership with other government agencies and technology companies. Visitors to

---

[15] *Available at* www.ftc.gov/bcp/ed/pubs/consumers/idtheft/idt04.pdf.

[16] The FCRA also provides identity theft victims with additional tools to recover from identity theft. For example, identity theft victims who provide police reports to a consumer reporting agency may obtain a seven-year fraud alert on their credit files, alerting potential users of their reports to exercise special vigilance in opening accounts in the consumers' names. In addition, victims may block fraudulent information on their credit files, obtain from creditors the underlying documentation associated with transactions that may have been fraudulent, and prohibit creditors from reporting fraudulent information to the consumer reporting agencies. *See* FCRA, 15 U.S.C. §§ 605A, 605B, 609(e), and 611.

[17] *Available at* www.OnGuardOnline.gov. A Spanish-language counterpart, Alerta En Linea, is available at www.AlertaenLinea.gov.

the site can download educational games and videos, learn more about specific topics, including phishing and social networking, and obtain useful tips and information in an interactive format.

The Commission directs its outreach to businesses as well.[18] It has developed a brochure and an online tutorial[19] that set out the key components of a sound data security plan. These materials alert businesses to the importance of data security and give them a solid foundation on how to address those issues. In addition, the FTC creates business educational materials to address particular risks. For example, the Commission developed a new business education brochure *Peer-to-Peer File Sharing: A Guide for Business*[20] to educate businesses about the risks associated with P2P file sharing programs and advise them about ways to address these risks.

Further, the Commission leverages its resources by providing educational and training materials to "first responders." For example, because victims often report identity theft to state and local law enforcement agencies, the FTC offers resources to law enforcers on how to talk to victims about identity theft.[21] The Commission also distributes a law enforcement resource CD Rom that includes information about how to assist victims, how to partner with other law enforcement agencies, how to work with businesses, and how to access the Identity Theft

---

[18] *See* FTC, *Protecting Personal Information: A Guide for Business;* and FTC, *Information Compromise and Risk of Identity Theft: Guidance for Your Business.* Both publications are available at http://business.ftc.gov.

[19] The tutorial is available at www.ftc.gov/bcp/edu/multimedia/interactive/infosecurity/index.html.

[20] *Available at* www.ftc.gov/bcp/edu/pubs/business/idtheft/bus46.shtm. Peer-to-Peer (P2P) technology enables companies to form a network in order to share documents and to facilitate online telephone conversations.

[21] Resources for law enforcement are available at www.ftc.gov/idtheft.

Clearinghouse. In addition, the FTC and its partners have provided identity theft training to over 5,400 state and local law enforcement officers from over 1,770 agencies.

Finally, the FTC has encouraged the development of a nationwide network of *pro bono* clinics to assist low-income identity theft victims. As part of this initiative, the FTC has created a comprehensive guide for advocates providing legal assistance to identity theft victims. The Guide for Assisting Identity Theft Victims (*Pro Bono Guide)*[22] describes how advocates can intervene with creditors, credit reporting agencies, debt collectors, and others, and it provides self-help measures that victims can take to address their problems. Step-by-step instructions provide best practices for recovering from identity theft.

III. CHILD IDENTITY THEFT

In addition to its general efforts to combat identity theft, the Commission often examines how to target its outreach efforts toward vulnerable populations, such as children who have been victims of identity theft. Through a variety of means, identity thieves may deliberately capture and use a child's SSN, or fabricate a SSN that coincidentally has been assigned to a child, in order to obtain employment, apply for government benefits, open new accounts, or apply for car loans or even mortgages. Indeed, one study has estimated that 142,000 instances of identity fraud are perpetrated on minors in the United States each year.[23] Another study of 40,000

---

[22] The *Pro Bono Guide* is available at www.idtheft.gov/probono.

[23] *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. ID Analytics noted, however, 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 service, and likely does not include instances of parents who may victimize their own children, nor does it reach all uses of child data for fraud (e.g., medical claims, government benefits, employment).

children who had been enrolled in an identity protection service found that 4,311 of those children or 10.2% had loans, property, utility, and other accounts associated with their SSNs.[24] Child identity theft is especially pernicious because the theft may not be detected until the child becomes an adult and seeks employment, or applies for student and car loans.

To help address the challenges raised by child identity theft, Commission staff, along with the Department of Justice's Office for Victims of Crime, recently hosted *Stolen Futures: A Forum on Child Identity Theft*.[25] Panelists, including educators, child advocates, legal services providers, and representatives of various governmental agencies and the private sector, discussed how to prevent and remedy child identity theft. Below is an overview of the discussions that took place at the forum and recommendations for next steps.

A. The Child Identity Theft Forum Discussions

First, panelists focused on the causes of child identity theft. They noted that identity thieves often steal children's information from schools, businesses, and government agencies. Panelists also noted that friends and family members may use children's identities, particularly when they fall on hard economic times.[26] Indeed, a lack of access to credit may cause family members including extended family members to use the identities of children in their

---

[24] *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.

[25] *See* 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.shtm.

[26] *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_.

households in order to pay basic expenses, such as heat and other utilities. In addition, several panelists noted that sensitive health and other personal information of children in foster care is often circulated widely within the schools and social services networks, leaving foster children particularly vulnerable to identity theft.[27]

Second, panelists discussed the unique challenges created by child identity theft. For example, a child's unused SSN is uniquely valuable to a thief because it typically lacks a previous credit history and can be paired with any name and birth date. In effect, a child's identity is a blank slate that can be used to obtain goods and services over a long time period because parents typically do not monitor their children's credit, often having no reason to suspect any problem.

In addition, while businesses can often detect instances of fraud involving adults by comparing an adult's SSN against a fraud or other commercial database, the same does not hold true for children, who typically lack an established credit history. Indeed, fraud alerts, a key tool used by adult victims of identity theft to warn potential creditors of possible identity theft, are premised on the existence of a credit file. Parents ordinarily cannot place a fraud alert on their child's credit file if the child has no such file.

Further, remedies available under federal law such as extended fraud alerts, access to documents underlying the theft, and blocking of erroneous debts typically require a victim to obtain a police report to document the crime. Panelists noted that children victimized by parents

---

[27] *See* Transcript of Stolen Futures, Session 1, Remarks of Matt Cullina, *available at* http://htc-01.media.globix.net/COMP008760MOD1/ftc_web/FTCindex.html#July12_.

or guardians are often reluctant to file a police report naming a loved one or a source of financial support as the perpetrator.[28]

Third, panelists discussed potential solutions to the problem. A representative from the Utah Attorney General's Office discussed a Utah initiative that would enable parents to enroll their child in a state identity protection program. Utah would pass the child's information onto TransUnion, which would in turn place a "high risk" alert on the child's name and SSN.[29] This program would help prevent an identity thief from attempting to obtain credit in the child's name or SSN. According to the Utah representative, Utah would like to work with other states to expand the program nationwide, once it is fully implemented.[30]

Private solutions were also discussed. Parents may enroll their children in a monitoring service to detect possible early signs of identity theft. One approach scans children's personal information to determine whether there are matches in various credit and other databases. Another approach provides alerts to parents if a child's personal information is being used in credit and other commercial transactions, such as a new credit application. Both of these approaches require additional investigation to confirm actual child identity theft because the use

---

[28] *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_.

[29] *See generally* Transcript of Stolen Futures, Session 4, Remarks of Richard Hamp, *available at* http://htc-01.media.globix.net/COMP008760MOD1/ftc_web/FTCindex.html#July12_.

[30] Mr. Hamp also explained that Utah has considered expanding the program to enable TransUnion to suppress erroneous information already existing in a child's file. However, the necessary steps to authenticate the child's identity appear to be cost-prohibitive at this time.

of a child's SSN could be an innocent mistake, such as the result of a transposed number. Panelists encouraged further study of these types of solutions.

Finally, panelists discussed the importance of prevention. Controlling and limiting access to a child's information is one of the best ways to protect children from identity theft, and panelists suggested several ways to do so. For example, panelists recommended that parents and guardians challenge requests for their child's SSN and other personal information. They should ask why information is being collected and how it is going to be used. Panelists also suggested that parents and guardians learn how their child uses the internet and social media, so that children do not divulge personal information that could be used to commit identity theft. As to child identity theft in the foster care system, panelists encouraged increased outreach to over-burdened case-workers, who may be unaware of the problem and do not know how to protect against it. They also encouraged increased outreach directly to foster youth, especially older teens who are soon to exit the foster care system. For example, one pilot program in California, the First Star UCLA Bruin Guardian Scholars Summer Academy, provides a free five-week curriculum that teaches foster youth various skills, including how to be their own advocates regarding their credit and personal information.[31] The organizers of this program, which currently serves thirty youths, hope to replicate it nationally.

B. Next Steps

The Commission's primary goal in co-hosting the forum was to learn more about the problem of child identity theft and to develop messages and target audiences for outreach on this issue. Based on the discussions from the forum, the Commission staff is preparing new

---

[31] *See* www.guardianscholars.ucla.edu/docs/Application%20Packet%202011.pdf.

educational materials in several areas. First, the staff is developing a "back-to-school alert," educating parents on the importance of safeguarding children's information in schools. The Commission staff has worked collaboratively with the Department of Education on this alert. Second, staff is working on new education materials for parents to be distributed widely through local and community organizations on how to prevent child identity theft, how to protect children's personal data, and how to help their children who have been victims of identity theft. Third, staff plans to conduct outreach to foster care advocates to find ways to better assist foster care youth both in protecting their personal data and in removing bad debts fraudulently incurred in their name. Fourth, staff plans to conduct outreach to social workers, legal services officials, and others who believe a child has been the victim of familial identity theft. Finally, staff plans to develop outreach materials specifically designed for young adults who learn that they have been identity theft victims. Commission staff remains open to additional approaches and will work with other federal and state agencies, private industry, and non-profit legal service providers and other organizations to develop outreach programs to combat child identity theft. Of course, in addition to targeting its outreach efforts, the agency will continue its robust efforts to address all forms of identity theft through law enforcement, partnerships with state and federal agencies, nationwide data management and analysis, and education.

IV. CONCLUSION

The Commission will continue to play a central role in the battle against identity theft, including child identity theft, and looks forward to working with you on this important issue.