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

[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

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.

[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

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 se

[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. These 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.

[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 rea

children who had been enrolled in an identity protection service found that 4,311 of those

[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_ .

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.

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.