

PREPARED STATEMENT OF
THE FEDERAL TRADE COMMISSION ON
IDENTITY THEFT: PREVENTION AND VICTIM ASSISTANCE

Before the
SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATIONS
of the
HOUSE COMMITTEE ON ENERGY AND COMMERCE

Langhorne, PA

December 15, 2003

I. INTRODUCTION

Mr. Chairman, and members of the Subcommittee, I am Betsy Broder, Assistant Director of the Division of Planning and Information, Bureau of Consumer Protection, Federal Trade Commission ("FTC" or "Commission").¹ I appreciate the opportunity to present the Commission's views on the impact of identity theft on consumers.

The Federal Trade Commission has a broad mandate to protect consumers, and controlling identity theft is an important issue of concern to all consumers. The FTC's role in combating identity theft derives from the 1998 Identity Theft Assumption and Deterrence Act ("the Identity Theft Act" or "the Act").² The Act directed the Federal Trade Commission to establish the federal government's central repository for identity theft complaints, to make available and to refer these complaints to law enforcement for their investigations, and to provide victim assistance and consumer education. Thus, the FTC's role under the Act is primarily one of facilitating information sharing among public and private entities.³ The Commission also works

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 Commissioner.

² Pub. L. No. 105-318, 112 Stat. 3007 (1998) (codified at 18 U.S.C. § 1028).

³ Most identity theft cases are best addressed through criminal prosecution. The FTC itself has no direct criminal law enforcement authority. Under its civil law enforcement authority provided by Section 5 of the FTC Act, the Commission may, in appropriate cases, bring actions to stop practices that involve or facilitate identity theft. *See, e.g., FTC v. Corporate Marketing Solutions, Inc.*, CIV - 02 1256 PHX RCB (D. Ariz. Feb. 3, 2003) (final order) (defendants "pretexted" personal information from consumers and engaged in unauthorized billing of consumers' credit cards) and *FTC v. C.J.*, CIV - 03 5275 GHK (RZx) (C.D. Cal. July 24, 2003) (final order) (defendant sent spam purporting to come from AOL and created an AOL look-alike website in order to obtain credit card numbers and other financial data from consumers which defendant used for unauthorized online purchases.). In addition, the FTC brought six complaints against marketers for purporting to sell international driver's permits that could be
(continued...)

extensively with industry on ways to improve victim assistance, including providing direct advice and assistance in cases of security breaches involving sensitive information of customers or employees.

II. THE FEDERAL TRADE COMMISSION'S ROLE IN COMBATING IDENTITY THEFT

The Identity Theft Act strengthened the criminal laws governing identity theft⁴ and focused on consumers as victims.⁵ In so doing, Congress recognized that coordinated efforts are essential to best serve the needs of identity theft victims because these fraud victims often need assistance both from government agencies at the national and state or local level and from businesses. To fulfill the Act's mandate, the Commission implemented a program that focuses on three principal components: (1) collecting complaints and providing victim assistance through a telephone hotline and a dedicated website; (2) maintaining and promoting the Identity Theft Data Clearinghouse (the "Clearinghouse"), a centralized database of victim complaints that serves as an

³ (...continued)

used to facilitate identity theft. Press Release, Federal Trade Commission, *FTC Targets Sellers Who Deceptively Marketed International Driver's Permits over the Internet and via Spam* (Jan. 16, 2003), available at <http://www.ftc.gov/opa/2003/01/idpfinal.htm>.

⁴ 18 U.S.C. § 1028(a)(7). The statute broadly defines "means of identification" to include "any name or number that may be used, alone or in conjunction with any other information, to identify a specific individual," including, among other things, name, address, social security number, driver's license number, biometric data, access devices (*i.e.*, credit cards), electronic identification number or routing code, and telecommunication identifying information.

⁵ Because individual consumers' financial liability is often limited, prior to the passage of the Act, financial institutions, rather than individuals, tended to be viewed as the primary victims of identity theft. Setting up an assistance process for consumer victims is consistent with one of the Act's stated goals: to recognize the individual victims of identity theft. *See* S. Rep. No. 105-274, at 4 (1998).

investigative tool for law enforcement; and (3) providing outreach and education to consumers, law enforcement, and private industry on prevention of identity theft.

A. Understanding Identity Theft

On November 1, 1999, the Commission began collecting complaints from consumers via a toll-free telephone number, 1-877-ID THEFT (438-4338) (“ID Theft hotline”). Every year since has seen an increase in complaints.⁶ The Clearinghouse now contains over 400,000 identity theft complaints from victims across the country. By itself, though, this self-reported data does not allow the FTC to draw conclusions about the incidence of identity theft in the general population. Consequently, the FTC commissioned a survey to get a better picture of the incidence of identity theft and the impact of the crime on its victims.⁷ The results are startling. Identity theft is more widespread and pernicious than previously realized. The data show that within the 12 months preceding the survey, 3.2 million people discovered that an identity thief opened new accounts in their name. An additional 6.6 million consumers learned of the misuse of an existing account. Overall, nearly 10 million people – or 4.6 percent of the adult population – discovered that they were victims of some form of identity theft. These numbers translate to nearly \$48 billion in losses to businesses, nearly \$5 billion in losses to victims, and almost 300 million hours spent by victims trying to resolve the problem. Moreover, according to the researchers, identity theft is a growing crime. The survey indicates a significant increase in the past 2-3 years – nearly a

⁶ Charts that summarize data from the Clearinghouse can be found at <http://www.consumer.gov/idtheft/stats.html> and <http://www.consumer.gov/sentinel/index.html>.

⁷ The research took place during March and April 2003. It was conducted by Synovate, a private research firm, and involved a random sample telephone survey of over 4,000 U.S. adults. The full report of the survey can be found at <http://www.consumer.gov/idtheft/stats.html>.

doubling from one year to the next, although the research shows that the rate of increase slowed during the past 1-2 years. It also is worth noting that most of the recent increase primarily involves the account takeover form of identity theft that tends to cause less economic injury to victims and is generally easier for them to identify and fix. Overall, the survey puts the problem of identity theft into sharper focus, and has spurred the FTC to even greater efforts to help victims and support law enforcement in its aggressive prosecution of identity thieves.

B. Assisting Identity Theft Victims

In addition to taking complaints from victims, the FTC provides advice on recovery from identity theft. Callers to the ID Theft hotline receive telephone counseling from specially trained personnel who provide general information about identity theft and help guide victims through the steps needed to resolve the problems resulting from the misuse of their identities.⁸ Victims are advised to: (1) obtain copies of their credit reports from the three national consumer reporting agencies and have a fraud alert placed on their credit reports;⁹ (2) contact each of the creditors or service providers where the identity thief has established or accessed an account, to request that the account be closed and to dispute any associated charges; and (3) report the identity theft to the police and get a police report, which is very helpful in demonstrating to would-be creditors and debt collectors that the consumers are genuine victims of identity theft.

⁸ Spanish speaking counselors are available for callers who are not fluent in English.

⁹ These fraud alerts indicate that the consumer is to be contacted before new credit is issued in that consumer's name. *See* Section II.D.(3)(b) *infra* for a discussion of the credit reporting agencies "joint fraud alert" initiative.

Counselors also advise victims having particular problems about their rights under relevant consumer credit laws including the Fair Credit Reporting Act,¹⁰ the Fair Credit Billing Act,¹¹ the Truth in Lending Act,¹² and the Fair Debt Collection Practices Act.¹³ If the investigation and resolution of the identity theft falls under the jurisdiction of another regulatory agency that has a program in place to assist consumers, callers also are referred to those agencies.

The FTC's identity theft website, located at www.consumer.gov/idtheft, provides equivalent service for those who prefer the immediacy of an online interaction. The site contains a secure complaint form that allows victims to enter their identity theft information for input into the Clearinghouse. Victims also can read and download all of the resources necessary for reclaiming their credit record and good name. One resource in particular is the FTC's tremendously successful consumer education booklet, *Identity Theft: When Bad Things Happen to Your Good Name*. The 26-page booklet, now in its fourth edition, comprehensively covers a range of topics, including the first steps to take for victims, how to correct credit-related and other problems that may result from identity theft, tips for those having trouble getting a police report taken, and advice on ways to protect personal information. It also describes federal and state resources that are available to victims who may be having particular problems as a result of the identity theft. The FTC alone has distributed more than 1.2 million copies of the booklet since its

¹⁰ 15 U.S.C. § 1681 *et seq.*

¹¹ *Id.* § 1666. The Fair Credit Billing Act generally applies to “open end” credit accounts, such as credit cards, revolving charge accounts, and overdraft checking accounts. It does not cover installment contracts, such as loans or extensions of credit that are repaid on a fixed schedule.

¹² *Id.* § 1601 *et seq.*

¹³ *Id.* § 1692 *et seq.*

release in February 2000, and recorded over 1.2 million visits to the web version.¹⁴ Last year, the FTC released a Spanish language version of the Identity Theft booklet, *Robo de Identidad: Algo malo puede pasarle a su buen nombre*.

C. The Identity Theft Data Clearinghouse

Because one of the primary purposes of the Identity Theft Act was for criminal law enforcement agencies to use the database of victim complaints to support their investigations, the Commission took a number of steps to ensure that the database would meet the needs of law enforcement, before launching it. Initially, the FTC met with a host of law enforcement and regulatory agencies to obtain feedback on what the database should contain. Law enforcement access to the Clearinghouse via the FTC's secure website became available in July of 2000. To ensure that the database operates as a national clearinghouse for complaints, the FTC has solicited complaints from other sources. For example, in February 2001, the Social Security Administration Office of Inspector General (SSA-OIG) began providing the FTC with complaints from its fraud hotline, significantly enriching the FTC's database.

The Clearinghouse provides a picture of the nature, prevalence, and trends of the identity theft victims who submit complaints. FTC data analysts aggregate the data and develop them into charts and statistics.¹⁵ For instance, the Commission publishes charts showing the prevalence of identity theft by states and by cities. Law enforcement and policy makers at all levels of government use these reports to better understand the challenges identity theft presents.

¹⁴ Other government agencies, including the Social Security Administration, the SEC, and the FDIC also have printed and distributed copies of *Identity Theft: When Bad Things Happen to Your Good Name*.

¹⁵ Charts that summarize data from the Clearinghouse can be found at <http://www.consumer.gov/idtheft/stats.html> and <http://www.consumer.gov/sentinel/index.html>.

Since the inception of the Clearinghouse, more than 770 law enforcement agencies, from the federal to the local level, have signed up for access to the database. Individual investigators within those agencies have the ability to access the system from their desktop computers 24 hours a day, seven days a week. The Commission actively encourages even greater participation.

As previously stated, one of the goals of the Clearinghouse and the FTC's identity theft program is to support identity theft prosecutions nationwide.¹⁶ Last year, in an effort to further expand the use of the Clearinghouse among law enforcement, the FTC, in cooperation with the Department of Justice, the United States Postal Inspection Service, and the United States Secret Service, initiated full-day identity theft training seminars for state and local law enforcement officers. To date, sessions have been held in Washington, D.C., Des Moines, Chicago, San Francisco, Las Vegas, Dallas, Phoenix, New York, Seattle, and San Antonio. The FTC also helped the Kansas and Missouri offices of the U.S. Attorney and State Attorney General conduct a training seminar in Kansas City. More than 1200 officers have attended these seminars, representing more than 300 different agencies. A session to be held in Orlando in January will commence next year's round of seminars.

The FTC staff also developed an identity theft case referral program.¹⁷ The staff creates preliminary investigative reports by examining significant patterns of identity theft activity in the

¹⁶ The Commission testified last year in support of S. 2541, the Identity Theft Penalty Enhancement Act of 2002, which would increase penalties and streamline proof requirements for prosecution of many of the most harmful forms of identity theft. *See* Testimony of Bureau Director J. Howard Beales, Senate Judiciary Committee, Subcommittee on Terrorism, Technology and Government Information (July 11, 2002). S. 2541 has been reintroduced in the 108th Congress as S. 153.

¹⁷ The referral program complements the regular use of the database by all law enforcers from their desktop computers.

Clearinghouse and refining the data through the use of additional investigative resources. Then the staff refers the investigative reports to appropriate Financial Crimes Task Forces and other law enforcers located throughout the country for further investigation and potential prosecution. The FTC is aided in this work by its federal law enforcement partners including the United States Secret Service, the Federal Bureau of Investigation, and the United States Postal Inspection Service who provide staff and other resources.

D. Outreach and Education

The Identity Theft Act also directed the FTC to provide information to consumers about identity theft. Recognizing that law enforcement and private industry each play an important role in the ability of consumers both to minimize their risk and to recover from identity theft, the FTC expanded its outreach and education mission to include these sectors.

(1) *Consumers*: The FTC has taken the lead in coordinating with other government agencies and organizations in the development and dissemination of comprehensive consumer education materials for victims of identity theft and those concerned with preventing this crime. The FTC's extensive consumer and business education campaign includes print materials, media mailings, and radio and television interviews. The FTC also maintains the identity theft website, which includes the publications and links to testimony, reports, press releases, identity theft-related state laws, and other resources.

To increase identity theft awareness for the average consumer, the FTC recently developed a new primer on identity theft, *ID Theft: What's It All About?*. This publication discusses the common methods of identity thieves, how consumers can best minimize their risk of being victimized, how to identify the signs of victimization, and the basic first steps for victims. Since

its release in May 2003, the FTC has distributed almost 268,000 paper copies, and over 15,000 web versions. With the detailed victim recovery guide, *Identity Theft: When Bad Things Happen to Your Good Name*, the publication helps to fully educate consumers.

(2) *Law Enforcement:* Because law enforcement at the state and local level can provide significant practical assistance to victims, the FTC places a premium on outreach to such agencies. In addition to the training described previously (*see supra* Section II.C.), the FTC staff joined with North Carolina's Attorney General Roy Cooper to send letters to every other Attorney General letting him or her know about the FTC's identity theft program and how each Attorney General could use the resources of the program to better assist residents of his or her state. The letter encouraged each Attorney General to link to the consumer information and complaint form on the FTC's website and to let residents know about the hotline, stressed the importance of the Clearinghouse as a central database, and described all of the educational materials that each Attorney General can distribute to residents. North Carolina took the lead in availing itself of the Commission's resources in putting together for its resident victims a package of assistance that includes the ID Theft Affidavit (*see* Section II.D.(3)(b)), links to the FTC website and www.consumer.gov/idtheft. Through this initiative, the FTC hopes to make the most efficient use of federal resources by allowing states to take advantage of the work the FTC already has accomplished and at the same time continuing to expand the centralized database of victim complaints and increase its use by law enforcement nationwide. Other outreach initiatives include: (i) Participation in a "Roll Call" video produced by the Secret Service, which has been sent to thousands of law enforcement departments across the country to instruct officers on identity theft, investigative resources, and assisting victims and (ii) the redesign of the FTC's

website to include a section for law enforcement with tips on how to help victims as well as resources for investigations.

(3) *Industry*: The private sector can help with the problem of identity theft in a number of ways. For instance, businesses can prevent identity theft by keeping their customers' or employees' sensitive information secure and out of the wrong hands. In addition, businesses can implement procedures to assist identity theft victims in the recovery process.

(a) Information Security Breaches: The FTC works with institutions that maintain personal information to identify ways to help keep that information safe from identity theft. Last year, the FTC invited representatives from financial institutions, credit issuers, universities, and retailers to an informal roundtable discussion of how to prevent unauthorized access to personal information in employee and customer records. The FTC will soon publish a self-assessment guide to make businesses and organizations of all sizes more aware of how they manage personal information and to aid them in assessing their security protocols.

As awareness of the FTC's role in identity theft has grown, businesses and organizations that have suffered compromises of personal information have begun to contact the FTC for assistance. For example, in the cases of TriWest¹⁸ and Ford/Experian,¹⁹ in which tens of thousands of consumers' files were compromised, the Commission gave advice on how to notify those individuals and how to protect the data in the future. To provide better assistance in these types of cases, the FTC developed a kit, *Information Compromise and the Risk of Identity Theft*:

¹⁸ Adam Clymer, *Officials Say Troops Risk Identity Theft After Burglary*, N.Y. TIMES, Jan. 12, 2003, § 1 (Late Edition), at 12.

¹⁹ Kathy M. Kristof and John J. Goldman, *3 Charged in Identity Theft Case*, LA TIMES, Nov. 6, 2002, Main News, Part 1 (Home Edition), at 1.

Guidance for Your Business, that will be posted on the identity theft website in the coming weeks.

The kit provides advice on which law enforcement agency to contact, business contact information for the three major credit reporting agencies, suggestions for establishing an internal communication protocol, information about contacting the FTC for assistance, and a detailed explanation of what information individuals need to know. The kit also includes a model letter for notifying individuals when their names and Social Security numbers have been taken.

Organizations are encouraged to print and include copies of *Identity Theft: When Bad Things Happen to Your Good Name* with the letter to individuals.

The FTC particularly stresses the importance of notifying individuals as soon as possible when information has been taken that may put them at risk for identity theft. They can then begin to take steps to limit the potential damage to themselves. For example, individuals whose Social Security numbers have been compromised, and who place a fraud alert promptly have a good chance of preventing, or at least reducing, the likelihood that the theft or release of this information will turn into actual misuse. Prompt notification also alerts these individuals to review their credit reports and to watch for the signs of identity theft. In the event that they should become victims, they can quickly take action to clear their records before any long-term damage is done. Besides providing *Information Compromise and the Risk of Identity Theft: Guidance for Your Business*, the FTC staff can provide individual assistance and advice, including review of consumer information materials for the organization and coordination of searches of the Clearinghouse for complaints with the law enforcement officer working the case.

(b) Victim Assistance: Identity theft victims spend significant time and effort restoring their good name and financial records. As a result, the FTC devotes significant

resources to conducting outreach with the private sector on ways to improve victim assistance procedures. One such initiative arose from the burdensome requirement that victims complete a different fraud affidavit for each different creditor with whom the identity thief had opened an account.²⁰ To reduce that burden, the FTC worked with industry and consumer advocates to create a standard form for victims to use in resolving identity theft debts. From its release in August 2001 through October 2003, the FTC has distributed more than 293,000 print copies of the ID Theft Affidavit. There have also been nearly 479,000 hits to the web version. The affidavit is available in both English and Spanish.

Another initiative designed to assist victims is the “joint fraud alert” administered by the three major credit reporting agencies (“CRAs”). After receiving a request from an identity theft victim for the placement of a fraud alert on his or her consumer report and for a copy of that report, each CRA now shares that request with the other two CRAs, thereby eliminating the requirement that the victim contact each of the three major CRAs separately.

III. New Protections for Identity Theft Victims

On December 4, President Bush signed the Fair and Accurate Credit Transactions Act of 2003.²¹ Many of the provisions amend the Fair Credit Reporting Act (“FCRA”)²² and provide

²⁰ See *ID Theft: When Bad Things Happen to Your Good Name: Hearing Before the Subcomm. on Technology, Terrorism and Government Information of the Senate Judiciary Comm.* 106th Cong. (2000) (statement of Mrs. Maureen Mitchell, Identity Theft Victim).

²¹ Pub. L. No. 108-396 (2003) (codified at 15 U.S.C. § 1681 *et seq.*).

²² 15 U.S.C. § 1681 *et seq.*

new and important measures to prevent identity theft, enhance consumer ability to detect it when it does occur, and facilitate identity theft victims' recovery.²³

A. Access to free consumer reports²⁴

Previously, under the FCRA consumers were entitled to a free consumer report only under limited circumstances.²⁵ Now consumers have the right to request a free consumer report annually from nationwide CRAs. This benefit will enhance consumers' ability to discover and correct errors, thereby improving the accuracy of the system, and also can provide an early alert to identity theft victims about crimes committed in their names.

²³ The Commission testified on July 9 and 10, 2003 before the House Committee on Financial Services and the Senate Committee on Banking, Housing, and Urban Affairs respectively. The testimony can be found at <http://www.ftc.gov/os/2003/07/fcratest.html> and <http://www.ftc.gov/os/2003/07/fcrasenatest.htm>.

²⁴ Pub. L. No. 108-396, § 211 (2003).

²⁵ Previously, free reports were available only pursuant to the FCRA when the consumer suffered adverse action, believed that fraudulent information may be in his or her credit file, was unemployed, or was receiving welfare benefits. Absent one of these exceptions, consumers had to pay a statutory "reasonable charge" for a file disclosure; this fee is set each year by the Commission and is currently \$9. *See* 15 U.S.C. § 1681j. In addition, a small number of states required the CRAs to provide free annual reports to consumers at their request.

B. National fraud alert system²⁶

Under this provision, consumers who reasonably suspect they have been or may be victimized by identity theft, or who are military personnel on active duty away from home, can place an alert on their credit files. The alert will put potential creditors on notice that they must proceed with caution when granting credit in the consumer's name. The provision also codified and standardized the industry's "joint fraud alert" initiative (*see* Section II.D.(3)(b) *supra*).

C. Identity theft account blocking²⁷

This provision requires CRAs immediately to cease reporting, or block, allegedly fraudulent account information on consumer reports when the consumer submits a police report or similar document, unless there is reason to believe the report is false. Blocking would mitigate the harm to consumers' credit records that can result from identity theft.

D. Truncation of credit and debit card receipts²⁸

In many instances, identity theft results from thieves obtaining access to account numbers on credit card receipts. This source of fraud could be reduced by requiring merchants to truncate the full card number on the receipt. The use of truncation technology is becoming widespread, and some card issuers already require merchants to truncate. This law now requires truncation of credit and debit card numbers on electronic receipts, but creates a phase-in period to allow for the replacement of existing equipment.

²⁶ Pub. L. No. 108-396, § 112 (2003).

²⁷ *Id.* § 152.

²⁸ *Id.* § 113.

E. “Red flag” indicators of identity theft²⁹

Under this provision, the banking regulators and the FTC will jointly develop guidelines for “red flag” indicators of identity theft. The goal of this provision is to give financial institutions and creditors up-to-date information on identity theft patterns and practices so that they can take appropriate action to prevent this crime.

IV. CONCLUSION

Identity theft places substantial costs on individuals and businesses. The Commission, through its education and enforcement capabilities, is committed to reducing identity theft as much as possible. The Commission will continue its efforts to assist criminal law enforcement with their investigations. Prosecuting perpetrators sends the message that identity theft is not cost-free. Finally, the Commission knows that as with any crime, identity theft can never be completely eradicated. Thus, the Commission’s program to assist victims and work with the private sector on ways to facilitate the process for regaining victims’ good names will always remain a priority.

²⁹ *Id.* § 114.