# PREPARED STATEMENT OF THE FEDERAL TRADE COMMISSION ON THE IDENTITY THEFT PENALTY ENHANCEMENT ACT OF 2002

#### Before the

#### SUBCOMMITTEE ON TECHNOLOGY, TERRORISM AND GOVERNMENT INFORMATION

of the

# SENATE JUDICIARY COMMITTEE Washington, D.C.

July 9, 2002

#### I. INTRODUCTION

Madam Chairman and members of the Committee, I am Howard Beales, Director of the Bureau of Consumer Protection, Federal Trade Commission ("FTC" or "Commission").(1) I appreciate the opportunity to present the Commission's views on the importance of strengthening the tools available to law enforcement as a means to both prevent and deter the crime of identity theft.

In March of this year, I had the opportunity to testify before this Subcommittee on the serious consequences that can result from identity theft. (2) In that testimony, I described three main components of the FTC's identity theft program: our Identity Theft Data Clearinghouse (the "Clearinghouse"); our consumer education and assistance resources, including our toll-free hotline, website, and educational brochures; and our collaborative and outreach efforts with law enforcement and private industry. Today, I would like to focus on the various ways the FTC works with law enforcement in order to facilitate their investigation and prosecution of identity theft crimes, and to express the Commission's support for the Identity Theft Penalty Enhancement Act, which will help achieve that goal.

The FTC has committed significant resources to assisting law enforcement, and fully intends to continue to do so in the future. Investigation and prosecution not only stop the offender from destroying another person's financial well being, but can also deter would-be identity thieves from committing the crime.

# II. The Identity Theft Penalty Enhancement Act - S. 2541

Since the enactment of the Identity Theft and Assumption Deterrence Act of 1998 ("Identity Theft Act")(3), we have learned more about how this pernicious crime works. Our colleagues in criminal law enforcement have seen how identity theft can further many types of financial fraud and even terrorism. The Identity Theft Penalty Enhancement Act, S. 2541, provides for enhanced charging and sentencing when identity theft occurs in connection with these other serious crimes. The Commission supports S. 2541 and its goal of increasing criminal penalties for the most damaging forms of identity theft.

The sentencing enhancements that S. 2541 envisions would, if enacted, step-up the penalties for the most serious forms of identity theft, and strengthen prosecutors' ability to bring these cases. In particular, the proposed legislation would define a new crime of "aggravated identity theft" that includes the most deleterious forms of identity theft, and which would carry greater penalties. Many of the predicate offenses that are included in the definition of "aggravated" identity theft, including identity theft for the purpose of defrauding employee benefit plans or committing bank

fraud, have predictably serious consequences to both the individual and institutional victims of the crime. Each of these would carry a two-year consecutive enhancement to the sentence. Enhanced five-year consecutive penalties would result if a terrorist or terrorist-related offense is involved.

S. 2541 also streamlines proof requirements by including the possession of identifying information with intent to commit identity theft as an element of the crime. These provisions, together with the enhanced sentences for aggravated identity theft, will make identity theft cases easier to investigate and to prosecute successfully.

#### III. The Complaint Clearinghouse

The Identity Theft Act directed the FTC to, among other things, log the complaints from victims of identity theft and refer those complaints to appropriate entities such as appropriate law enforcement agencies. Before launching our complaint system, the Commission took a number of steps to ensure that it would meet the needs of criminal law enforcement. For example, in April 1999, representatives from ten federal law enforcement agencies, five banking regulatory agencies, the US Sentencing Commission, the National Association of Attorneys General and the New York State Attorney General's Office met at the FTC to share their thoughts on what the FTC's complaint database and comprehensive consumer education booklet should contain. The roundtable participants also established a working group that provided feedback throughout the construction of the database. The FTC opened the consumer hotline and began adding complaints to the resulting Clearinghouse in November 1999. Law enforcement organizations nationwide who were members of our Consumer Sentinel Network (the FTC's universal fraud complaint database) gained access to the Clearinghouse via our secure Web site in July of 2000.

To ensure that the database operates as a national clearinghouse for complaints, the FTC has solicited complaint entry from other critical sources. For example, in November 2000, the International Association of Chiefs of Police (IACP) unanimously passed a resolution in support of curbing identity theft that, among other things, calls upon local police to refer identity theft victims to the FTC's hotline so that their complaints will be available to law enforcement officers nationwide through the Clearinghouse. In February 2001, the Social Security Administration Office of Inspector General (SSA-OIG) began providing the FTC complaints from its fraud hotline, significantly enriching our database. As a result of these efforts, the Clearinghouse has become a key element in identity theft investigations.

Many of the agencies that collaborated on the development of the Clearinghouse also participate in the Attorney General's White Collar Crime Task Force's Subcommittee on Identity Theft. Subcommittee members and other Consumer Sentinel users have told the FTC that the Clearinghouse is used primarily in two ways: to initiate new investigations, and even more often, to identify additional victims, suspects, addresses, phone numbers and criminal activities related to an ongoing investigation.

The Clearinghouse provides a much fuller picture of the nature, prevalence, and trends of identity theft than was previously available. (4) In 2000, our first full year of operation, we entered more than 31,000 consumer complaints into the database. In 2001, that number grew to 86,168. As of the end of May this year, only five months into the calendar year, 55,000 complaints have already been added to the database. These numbers reflect complaints only, and do not include the tens of thousands of consumers who contacted us with questions on how to prevent identity theft or how to handle the loss or theft of a purse or wallet. This growth means that the Clearinghouse will continue to become a richer source of data for law enforcement, both in terms of developing and enhancing cases, and in providing information about the overall patterns and trends in identity theft.

Data from the Clearinghouse also assist law enforcement in other important ways. FTC data analysts aggregate the data to develop statistics about the nature and frequency of identity theft. Law enforcement and other policy makers at all levels of government use these reports to better understand the challenges identity theft presents. For instance, we publish charts showing the prevalence of identity theft by states and by cities. The data also demonstrate general trends. The first twelve months of data revealed that over thirty-five percent of victims who called us reported that they had not been able to file police reports. Following the November 2000 IACP resolution that called upon local police to write reports for all incidents of identity theft, the number of victims who were unable to file a report fell by almost half to eighteen percent.

Since the inception of the Clearinghouse, forty-six separate federal agencies and three hundred and six different state and local agencies have signed up for access to the database. Among the agencies represented are over half the state Attorneys General as well as law enforcement from a number of major cities including Baltimore, Dallas, Los Angeles, Miami, San Francisco, and Philadelphia. We want to encourage even greater participation. To that end, since March of this year, we have been conducting outreach and law enforcement training and demonstrating the efficacy of the Clearinghouse at law enforcement conferences around the country. We have seen positive results from these efforts. For example, within three weeks after our training seminar in Chicago, held this May, approximately a third of the participating agencies without prior access to the Clearinghouse had signed up, and we continue to receive applications. As a core component of our program, we will continue to focus resources and to devise new methods for expanding law enforcement access to the database.

# III. Partnership with the Secret Service

The Clearinghouse is essentially a tool for criminal investigators and prosecutors. The US Postal Inspection Service(5), the United States Secret Service (the "Secret Service") the SSA-OIG, the Department of Justice (DOJ), and the IACP, along with many other agencies, are outstanding partners in this effort, consistently communicating the availability and advantages of the Clearinghouse to their colleagues.

The Secret Service has made a particularly strong commitment to making the Clearinghouse the centralized investigatory tool for identity theft crimes nationwide. The Secret Service has just begun its second year of detailing a Special Agent to the FTC's identity theft program. This partnership has provided numerous benefits. In addition to the day-to-day assistance of an experienced law enforcement officer with expertise in investigating identity theft crimes, the Secret Service has also provided the FTC with access to powerful data mining and clustering software tools, the research capabilities provided by its financial crimes analysts, and its network of task forces throughout the country.

# A. Investigative Referrals

The Clearinghouse, which now contains over 170,000 victim complaints, can be searched with more precision using the Secret Service's data mining and clustering software tools. Taking the results of a search, the Special Agent works with FTC staff to develop the most significant case leads into full investigative reports. As part of that effort, the Secret Service runs the leads through the additional intelligence databases it uses in its own criminal investigations. Since last June, we have been referring the investigative reports to Financial Crimes Task Forces or other appropriate law enforcement entities. In other instances, law enforcement agents from around the country directly contact the FTC with requests for an enhanced database search on a lead they currently have under investigation.

# **B. Law Enforcement Training**

Recognizing that investigating identity theft often presents unique challenges, the FTC in conjunction with the Secret Service, DOJ, and IACP planned and directed training seminars for state and local law enforcement around the country in Washington, DC, Des Moines, Iowa, Chicago, Illinois, and in San Francisco. More than 440 people from over 100 different government departments and agencies have attended these seminars since we began them in March. Over three-quarters of the attendees were from state and local law enforcement and prosecuting authorities. An additional training program is planned for Dallas, Texas on August 14.

The training is designed to provide officers with technical skills and resources to enhance their efforts to combat identity theft. The training draws on the talent of local police and prosecutors, in addition to the core training staff from the FTC, DOJ and the Secret Service. While particular details may vary between venues, we stress two basic elements in the first half of the day: the value of Task Forces and the utility of the Clearinghouse to build and augment cases. The training also touches on the consumer educational and informational aspects of the FTC's identity theft program, because many law enforcement departments use our booklet, When Bad Things Happen To Your Good Name, as part of their victim assistance effort.

The training then moves to segments providing practical advice and demonstrating hands-on tools to help improve investigational strategies. In addition, presentations are geared towards familiarizing the attendees with the many different resources available to them from the federal, state and local government, and also from private industry, for investigating identity theft. Local prosecutors identify the key components they are looking for to bring successful identity theft actions. The feedback we have received has been very positive, and has enabled us to fine-tune each subsequent seminar.

#### IV. CONCLUSION

The Commission supports S. 2541, the Identity Theft Penalty Enhancement Act of 2002, and embraces its goal of increasing the prosecution and criminal penalties when the identity theft facilitates particularly pernicious crimes. When these crimes are committed under someone else's identity, it stigmatizes an innocent person who must struggle to clear his or her name from association with an exceptionally horrific misdeed. It is only just that such a crime should carry an additional penalty. The FTC will continue to do its part to support the prevention, investigation, prosecution and mitigation of identity theft by providing law enforcement with education, training, access to the Clearinghouse, and case referrals.

#### **Endnotes:**

- 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. See Testimony of J. Howard Beales, Senate Judiciary Committee, Subcommittee on Technology, Terrorism and Government Information (March 20, 2002).
- 3. Pub. L. No. 105-318, 112 Stat. 3010 (1998).
- 4. Attached are charts that summarize 2001 data from the Clearinghouse. These data are posted at <a href="www.consumer.gov/idtheft">www.consumer.gov/idtheft</a> and <a href="www.ttc.gov/sentinel">www.ttc.gov/sentinel</a>.
- 5. The Postal Inspection Service was the first agency to detail a law enforcement officer to work with the FTC's data sharing program. The Inspection Service detailed an inspector who, for over one year, managed our Consumer Sentinel system. These partnerships allow us to share expertise and also maintain open and ongoing communication.