Testimony of

# Chris Swecker

Assistant Director for the Criminal Investigative Division
Federal Bureau of Investigation
April 13, 2005

Testimony By
Chris Swecker
Assistant Director, Criminal Investigative Division
Federal Bureau of Investigation
Before the
Senate Judiciary Committee
April 13, 2005

"Securing Electronic Personal Data:
Striking a Balance Between
Privacy and Commercial and Governmental Use."

Good morning Mr. Chairman and members of the Committee. I want to thank you for the opportunity to testify before you today about the FBI's efforts to combat Identity Theft, as well as the FBI's use of public source data.
The FBI views identity theft as a significant and growing crime problem, especially as it relates to the theft of consumer information from large wholesale data companies.
The FBI opened 1,081 investigations related to identity theft in fiscal 2003 and 889 in fiscal 2004. That number is expected to increase as identity thieves become more sophisticated and as the technique is further embraced by large criminal organizations, placing more identity theft crime within FBI investigative priorities. At present, the FBI has over 1,600 active investigations involving some aspect of identity theft. These cases are tracked utilizing a crime problem indicator code.
The FBI does not specifically track identity theft convictions and indictments, as identity theft crosses all program lines and is usually perpetrated to facilitate other crimes such as credit card fraud, check fraud, mortgage fraud, and health care fraud.

Armed with a person's identifying information, an identity thief can open new accounts in the name of a victim, borrow funds in the victim's name, or take over and withdraw funds from existing accounts of the victim, such as their checking account or their home equity line of credit. Although by far the most prevalent, these financial crimes are not the only criminal uses of identity theft information, which can even include evading detection by law enforcement in the commission of violent crimes. Identity theft takes many forms, but generally includes the acquiring of an individual's personal information such as Social Security number, date of birth, mother's maiden name, account numbers, address, etc., for use in criminal activities such as obtaining unauthorized credit and/or bank accounts for fraudulent means.
Identity theft has emerged as one of the dominant white collar crime problems of the 21st Century. Estimates vary regarding the true impact of the problem, but agreement exists that it is pervasive and growing. In addition to the significant harm caused to the monetary victims of the frauds, often providers of financial, governmental or other services, the individual victim of the identity theft may experience a severe loss in their ability to utilize their credit and their financial identity. This loss can be short in duration, or may extend for years. It may result in the inability to cash checks, obtain credit, purchase a home or, in the most insidious cases, the arrest of the individual for crimes committed by the identity thief.
A May 2003 survey, commissioned by the Federal Trade Commission (FTC) estimated the number of consumer victims of identity theft over the year prior to the survey at 4.6% of the population of U.S. consumers over the age of 18, or 9.91 million individuals with losses totaling $52.6 billion. However, over half of these victims experienced only the take-over of existing credit cards which is generally not considered identity theft. New account frauds, more generally considered to be identity theft, were estimated to have victimized 3.23 million consumers and to have resulted in losses of $36.7 billion.

The FBI's Cyber Division also investigates instances of identity theft which occur over the Internet, or through computer intrusions by hackers.

In recognition of this fact, and the overriding need to gather the most complete and accurate intelligence as quickly as possible the FBI has focused its efforts on developing joint investigative initiatives with our partners in law enforcement, as well as key Internet E-commerce stake holders. These initiatives have targeted escalating cyber crimes, both domestically and internationally, and invariably included numerous incidents which could be characterized as Identity Theft.
The Internet Crime Complaint Center, otherwise known as IC3, is a joint project between the FBI and the National White Collar Crime Center. This joint collaboration serves as a vehicle to receive, develop, and refer criminal complaints regarding the rapidly expanding arena of cyber crime. The IC3 receives on average more than 17,000 complaints every month from consumers alone and additionally receives a growing volume of referrals from key E-commerce stakeholders. Of the more than 400,000 complaints referred to the IC3 since its opening in May of 2000, more than 100,000 were either characterized as Identity Theft, or involved conduct that could be characterized as Identity Theft.
It should be noted that Identity Theft in its many forms is a growing problem and is manifested in many ways, including large scale intrusions into third party credit card processors, theft from the mails of printed checks, pre-approved credit card offers and mortgage documents, credit card skimming, Phishing schemes, and telephone and bank frauds, much of which is perpetrated through the use of SPAM e-mail.

The FBI is developing cooperative efforts to address the identity theft crime problem. In cities such as Detroit, Chicago, Memphis and Mobile, task forces are currently operating in conjunction with other federal, state and local authorities as well as with affected merchants. In cities such as Tampa, San Diego and Philadelphia, efforts are underway to create or expand identity theft working groups and task forces. In addition, the FBI is focusing analytical resources on identity theft, working with other agencies, such as the FTC, to obtain identity theft data and utilize it to proactively identify and target organized criminal groups and enterprises.
Computer intrusions, or hackers, can significantly contribute to the impact and scope of Identity Theft.
Breaches of security at large providers of public source data have recently highlighted the ability of criminals to exploit the availability of data.
? In September 2004, Phillip A. Cummings pled guilty in U.S. District Court, Southern District of New York, to charges related to his role in the theft of over 30,000 consumer credit histories from 2000 to 2002.
Cummings was an employee of Teledata Communications, Inc. (TCI) which provided customers with computerized access to the three major commercial credit bureaus: Equifax, Experian, and Trans Union. Cummings had access to confidential passwords and subscriber codes and used the information to download consumer credit histories which he then sold to several individuals, some of whom used the information to obtain credit cards and merchandise. Losses to financial institutions in this case exceeded $11 million.
Cummings was sentenced to 14 years in federal prison and ordered to forfeit $1 million in illegal proceeds. This investigation was worked jointly with the United States Postal Inspection Service.

In January 2003, a counterfeit check ring utilizing the identity of Richard Johnson and the company name NEXTEL (with no connection to the real corporation of that name) opened an account with ChoicePoint. Utilizing stolen names and social security numbers, the ring utilized ChoicePoint to obtain over 100 credit reports for those identities. Derrick Grayson and Robert Stewart, the leaders of that ring, and nine others, have been convicted of crimes in connection with the counterfeit check ring. Grayson was sentenced to 130 months in prison based on his cooperation in the investigation. Stewart was sentenced to 190 months imprisonment.
? On 09/01/2004, Richard Burley and others were charged in U.S. District Court, Eastern District of Michigan, on bank fraud and conspiracy charges for their alleged roles in an identity theft ring which derived profits of more than $2 million. This indictment was the result of the investigative efforts of the Detroit Metro Identity Fraud Task Force (DMIFTF). The DMIFTF comprises agents from the FBI, U.S. Postal Inspection Service, United States Secret Service, the Michigan State Police, and several local police departments. Since its inception in 1999, the DMIFTF has accounted for more than 100 convictions for identity theft- related crimes.

? In October 2004, ChoicePoint detected fraudulent activity in several small business accounts based in the Los Angeles, California area. In coordination with the Los Angeles Sheriff's Department (LASD), ChoicePoint arranged a controlled delivery of documents. During the controlled delivery, Olatunji Oluwatosin was arrested. The investigation determined that Oluwatosin was associated with at least 23 ChoicePoint customer accounts. Oluwatosin has pled guilty to the charges and has been sentenced to 16 months in prison. Investigation related to this activity is

ongoing. The investigations stemming from these customer accounts are assigned to a Los Angeles County Sheriff's Deputy and a U.S. Postal Inspector who are members of the Identity Theft Task Force sponsored by their respective agencies and of which the FBI's Los Angeles Field Office is a member. The FBI SA assigned to the Identity Theft Task Force has not been tasked
with this particular investigation.

These breaches illustrate the ability of criminals to obtain the type of access to these data providers which is normally reserved for clients with legitimate business purposes for the use of the information. It is important to note that these represent a failure of the customer intake and authentication systems of the data providers, rather than a failure of the security of the data networks. In other words, these criminals were not permitted to access data in a manner that is inconsistent with that which is afforded legitimate businesses on a daily basis.
InfraGard is an FBI program that began in the Cleveland Field Office in 1996 as a local effort to gain support from the information technology industry and academia for the FBI's investigative efforts in the cyber arena. Today InfraGard has expanded to all FBI Field Offices with approximately 15,000 members ranging from representatives of Fortune 500 Companies to the owners of small Internet Service Providers. The membership represents a cross-section of the nation's critical infrastructures: Agriculture, Banking and Finance, Chemical Industry, College and Universities, Defense Industrial Base, Emergency Services, Energy, Food, Government, Postal and Shipping, Public Health, Information and Technology, Telecommunications, Transportation, and the Water Supply.

At its most basic level, InfraGard is a cooperative undertaking dedicated to sharing information and intelligence, to include issues involving possibly Identity Theft, derived from various FBI cyber related investigations. InfraGard provides a forum for dialogue and relationship building between policy makers, private companies, and the law enforcement community on a number of issues. Its goal is to enable a two way information flow so that the owners and operators of systems and networks can better protect themselves, and, as a result, the United States Government can better discharge its law enforcement and national security responsibilities. Information sharing is accomplished by InfraGard Chapters, which are geographically linked with FBI Field Office territories and their FBI Special Agent Coordinators.
The InfraGard membership regularly provides intelligence and referrals that assist law enforcement's efforts to identify and counter the most significant criminal and national security threats to our country's networks.
To assist in the development of the types of cases that necessitate federal treatment, the FBI is developing financial crimes intelligence related to identity theft. The FBI utilizes analysts to review information contained in suspicious activity reports, the Federal Trade Commission's Identity Theft Clearinghouse, fraud reporting to the Internet Crime Complaint Center and other sources of data to identify and target criminal organizations engaged in identity theft.

Choicepoint, like LexisNexis and the other available data resources, has become an invaluable research tool for the FBI's analytical cadre in a number of ways. Choicepoint consolidates a large number of public information sources in a single, online location for quick retrieval. Much of the information provided by Choicepoint could only be obtained historically by making direct and sometimes in-person contact with the originating Agency. Information from Choicepoint is used to provide useful leads for analysts and investigators to follow through on and can be integral in helping to draw connections between previously segregated pieces of data. The Choicepoint information is used regularly by investigators in contributing to probable cause for search warrants, court orders and other legal documents that are executed every day by FBI Agents.
An example of how Choicepoint can and has been used in analytical research can be seen in several of its search parameters. When the FBI has initiated an investigation, Choicpoint, through name and address information, can provide social security information on search projects. Once a social security number is available, analysts can enter this information into a new search parameter. These searches will produce all names that have ever been associated with the number. Many times, the production of these aliases can be used to run additional searches, providing even more potential leads for investigators to pursue. The automation of this multiple-source data, as with similar analytical engines, has dramatically reduced the amount of time and effort needed to include or exclude information.

The Choicepoint search engines also provide the names of potential family relatives and co-habitant data for subjects and subject addresses. When used with other informational databases, including the Bureau's internal indices, potential and concrete links can be established between multiple facets of an investigation, and often assist analysts in developing links between previously unconnected investigations. As criminals and criminal organizations become more complex, need reasonable access to potential source of data and information that might afford them the opportunity to establish these types of links which are crucial to realizing the entire scope of an investigation. Choicepoint information is not considered in a vacuum. It is one of many investigative tools which are used in law

enforcement by investigators and analysts. As with any source of information, it is considered in its relation to the totality of available information. It is particularly useful in that it allows analysts to inductively and deductively develop information about subjects, their confederates, witnesses and corporations that are associated with an investigation. Once again, I appreciate the opportunity to come before you today and share the work that the FBI has undertaken to address the problem of Identity Theft. The FBI's efforts in this arena will continue, and we will continue to keep this Committee informed of our progress in protecting America's citizens and economy.