Identity Theft: Victim's Bill of Rights Congressional Subcommittee Hearing

The Center for Identity Management and Information Protection (CIMIP) Participates in a Congressional Subcommittee Hearing on Identity Theft Victims.
Written by Ingrid Norris

On June 17, 2009 CIMIP's executive director, Don Rebovich, Ph.D., testified before a subcommittee of the Congressional Committee on Oversight and Government Reform. This committee is the main investigative committee in the U.S. House of Representatives. According to the Committee's Rules and Jurisdiction, the Congressional Committee has jurisdiction to investigate any federal program and any matter with federal policy implications.

The Congressional Committee is made up of five standing subcommittees represented by appropriate party ratios. These subcommittees are: Domestic Policy; Federal Workforce, Postal Service, and the District of Columbia; Government Management, Organization, and Procurement; Information Policy, Census, and National Archives; and National Security and Foreign Affairs.

Dr. Rebovich testified before the Subcommittee on Information Policy, Census, and National Archives. This subcommittee has oversight jurisdiction over public information and records laws such as the Freedom of Information Act, the Presidential Records Act, the Federal Advisory Committee Act, The Census Bureau, and the National Archives and Records Administration.

The members of Congress serving in the Subcommittee on Information Policy, Census, and National Archives are: William Lacy Clay (D), Missouri, Chairman; Paul Kanjorski (D), Pennsylvania; Carolyn Maloney (D), New York; Eleanor Holmes Norton (D), District of Columbia; Danny Davis (D), Illinois; Steve Driehaus (D), Ohio; Diane Watson (D), California; Patrick McHenry (R), North Carolina; Ranking Member, Lynn Westmoreland (R), Georgia; Vice Ranking Member John Mica (R), Florida, and Jason Chaffetz (R), Utah.

This year, the subcommittee held hearings on a wide range of topics. These topics included: *Cybersecurity: A Review of Public and Private Efforts to Secure our Nation's Internet Infrastructure*; *Examination of the State of Organ Donation*; *Census Data and its Use in the Development Process*; and *Joint Hearing on Federal IT Security: The Future of FISMA.*

The Subcommittee on Information Policy, Census, and National Archives hearing held on June 17 was titled *Identity Theft: Victims Bills of Rights.* The hearing was held for the purpose of examining the actions the federal government has taken to address the problem of identity theft and how to provide protection to victims of identity theft.

The chairman of the subcommittee, Wm. Lacy Clay, noted that the hearing was also conducted in response to concerns voiced by the public due to the vast number of problems that identity crime victims run into when trying to restore their identity. The problem, experts have said, is that identity theft prevention and assistance efforts are lagging far behind the needs of victims. Furthermore, the Chairman noted, identity thieves are quick to overcome any obstacles set in place by legislation.

To address concerns voiced by the public and in collaboration to combat and prevent identity theft, three topics were addressed at the hearing. These topics are: 1) Current and emerging

issues of identity theft. 2) How to improve both public and private assistance efforts to victims of identity theft. 3) How to increase prosecution and deterrence of identity thieves.

Members of Congress serving in the Subcommittee on Information Policy, Census, and National Archives invited public and private organizations to provide input and recommendations on these three topics. To accomplish this, the hearing was divided into two panels.

Panel One

The first panel consisted of three government agencies, the individuals that provided testimonies were: Betsy Broder, Assistant Director of the Division of Privacy and Identity Protection of the Federal Trade Commission (FTC); Jason Weinstein, Deputy Assistant Attorney General, Criminal Division of the U.S. Department of Justice (DOJ), and Daniel Bertoni, Director of Education, Workforce, and Income Security Issues of the Government Accountability Office (GAO).

Topic One: Current and Emerging Issues of Identity Theft

The following were some of the major current and emerging issues of identity theft issues noted by individuals in the first panel in their written testimony:

Betsy Broder noted that since 2001, the FTC used its authority to bring 26 cases against businesses for failure to 1) comply with posted privacy policies; 2) take even the most basic steps to protect against common technology threats; 3) dispose of data properly; and/or 4) take reasonable steps to ensure that they do not share customer data with unauthorized third parties.

Jason Weinstein noted that in cases where there was a breach in corporate databases where individuals or financial information was taken, not only do the affected individuals suffer the monetary losses they incur as a result, but the affected businesses bear the indirect costs of fraud prevention and mitigation of the harm, including potentially significant reputational harm.

Mr. Weinstein also indicated that many of the identity theft cases the Department of Justice prosecuted demonstrated that a single criminal can cause extensive harm to many individuals. As an example, Mr. Weinstein mentioned a case prosecuted by the USAO for the Middle District of Tennessee, where one defendant victimized over 100 people, repeatedly, using the stolen identities of minor children, the homeless, and others to place multiple fraudulent loans on the same property without the knowledge or consent of the true owners.

Daniel Bertoni noted that some public record keepers sell records containing Social Security Numbers (SSN) in bulk to private companies and provide access to records on their own government web sites. When records are sold in bulk or made available on the Internet, Mr. Bertoni explained, it is unknown how and by whom the records, and the personal identifying information contained in them, are used.

Mr. Bertoni further mentioned that GAO reported that an estimated 42 million Medicare cards, 8 million Department of Defense (DOD) insurance cards, and 7 million Department of Veterans Affairs (VA) beneficiary cards displayed entire 9-digit SSNs. Although efforts have been made to remedy this problem, Mr. Bertoni noted, the Centers for Medicare and Medicaid Services,

with the largest number of cards displaying the entire 9-digit SSN has no plans to remove the Social Security Numbers from Medicare identification cards.

Topic Two: Improvement of Public and Private Assistance Efforts to Victims of Identity Theft

The following were some of the recommendations made by individuals in the first panel, in their written testimonies, on how public and private assistance efforts to victims of identity theft can be improved:

Betsy Broder noted that for the public sector, the President's Identity Theft Task Force, co-chaired by the FTC, launched a variety of initiatives aimed at making the federal government a better custodian of sensitive personal information. As an example, Ms. Broder mentioned the following initiatives: 1) the Office of Management and Budget (OMB) issued data security and breach management guidance for government agencies; 2) The Social Security Administration removed Social Security Numbers (SSNs) almost entirely from its internal human resources forms; and 3) the Department of Defense (DOD) is working toward removal of SSNs from military identification cards.

Ms. Broder also mentioned that the FTC and other agencies are educating consumers on how to avoid becoming victims of identity theft. As an example Ms. Broder indicated that the FTC launched a nationwide identity theft education program titled "Avoid ID Theft: Deter, Detect, Defend" that contains a consumer education kit that includes direct-to-consumer brochures, training materials, presentation slides, and videos for use by such groups.

Jason Weinstein noted that the Department of Justice's Office for Victims of Crime (OVC) conducted a national training session, developed in cooperation with the FTC, for victim-witness coordinators in 2007. To increase identity theft victim assistance services, Mr. Weinstein noted, OVC has encouraged victim assistance administrators from the Victims of Crime Act (VOCA) to expand their program outreach to identity theft victims. Mr. Weinstein further noted that OVC has also highlighted identity theft and fraud issues at the VOCA Administrators' Annual Conferences by supporting victim impact workshops to help recognize the needs of identity theft victims and expand program services using VOCA victim assistance dollars.

Daniel Bertoni noted that the Department of Veterans Affairs (VA) and the Department of Defense (DOD) begun taking actions to remove SSNs from cards. As an example Mr. Bertoni cited VA's elimination of the use of SSNs from 7 million VA identification cards. VA plans to replace existing cards that show SSNs with cards that do not show SSNs; newly issued cards will not display SSNs.

Mr. Bertoni further mentioned that following GAO's recommendation, the 110th Congress enacted legislation to develop a standardized method for truncating SSNs. Truncation, Mr. Bertoni explained, is the practice of only displaying a partial number, such as the first 5 digits of a Social Security Number.

Mr. Bertoni also indicated that the Office of Management and Budget (OMB) directed agencies to encrypt data on mobile computers or devices and to follow the National Institute of Standards and Technology (NIST) security guidelines regarding personally identifiable information. Mr.

Bertoni explained that this approach reinforces compliance with the Privacy Act and the Federal Information Security Management Act of 2002 (FISMA)'s requirement to protect personally identifiable information.

Topic Three: Methods to Increase prosecution and Deterrence of Identity Thieves

The following were some of the recommendations made by members of the first panel, in their written testimony, on how to increase prosecution and deterrence of identity thieves:

Betsy Broder recommended that Congress provide the FTC with authority to seek civil penalties when dealing with data security cases. Such authority, Ms. Broder explained, would serve as an additional incentive for businesses to maintain reasonable data security measures.

Jason Weinstein urged Congress to consider requiring immediate security breach reports to federal law enforcement using a mechanism that ensures that the U.S. Secret Service and the FBI have access to private and public organization's breach of data reports. Mr. Weinstein explained that this requirement will enhance law enforcement's ability to promptly investigate large-scale data breaches.

Panel Two

Along with the Center for Identity Management and Information Protection (CIMIP), the other private organizations in the second panel consisted of Catherine Allen, Chairman and CEO of The Santa Fe Group; Marc Rotenberg, Executive Director of the Electronic Privacy Information Center (EPIC); Anne Wallace, President of the Identity Theft Assistance Corporation (ITAC); and Eric Handy, personal representative of Linda Goldman-Foley, founder of the Identity Theft Resource Center (ITRC).

Topic One: Current and Emerging Issues of Identity Theft

The following were some of the major current and emerging issues of identity theft issues noted by individuals in the second panel in their written testimony:

Catherine Allen noted that various studies indicated the expense identity theft victims go through to restore their credit can range from zero to $950. The time spent to restore their credit, Ms. Allen noted, can take from four to 165 hours. In many instances Ms. Allen went on to say, many identity theft victims have their credit card applications denied or their loans denied due to bad credit caused by the identity thief's actions.

In cases of medical identity theft, Ms. Allen noted, false information may become part of a person's medical record which can potentially endanger that person's health. The problem lies, Ms. Allen explains, with some medical institutions' belief that the Health Insurance Portability and Accountability Act (HIPPA) privacy protection rule applies even if the patient was treated under a false identity. This misinterpretation restricts identity theft victims from correcting his/her medical records.

Ms. Allen further noted that children's identities have been known to have been stolen before they're old enough to write their own names. The problem lies, Eric Handy explains, in the

current policy of issuing Social Security Numbers (SSNs) to minors, including infants. If the crime is undetected by parents, Mr. Handy further explained, it may create an unrestricted 18 year window of opportunity for identity thieves. The true recipient of the SSN may not even be aware of the situation until he/she applies for his/her first line of credit at which time it becomes the victim's burden to prove who he/she is.

Catherine Allen also noted that if criminal acts are committed under a stolen identity, the first news a victim often has of the identity theft may be when he or she is arrested. When this occurs, Eric Handy explained, a booking record is created that filters through a system not designed to be altered, or designed to allow for the removal of records. At this point, Ms. Allen explained, the victim must go through a "reverse booking" process that requires the person to prove his or her innocence.

Some law enforcement processes are not always in place, Ms. Allen noted, so when victims try to file a police report, they may be told they don't need to file a report or they need to talk to one or more additional departments. The problem, Anne Wallace explained, lies in gaps in resources and lack of training that limit the investigation and prosecution of many identity crimes. As a result, Ms. Allen explained, some identity crimes are treated as misdemeanors or very low-level felonies. The majority of prosecutions are dealt in civil courts preventing identity thieves from having a criminal record.

Another current and emerging issue of identity theft noted by Ms. Allen was that many individual identity crimes fall below the financial threshold that would trigger federal, state, or even local law enforcement agencies to act. Some businesses won't pursue or prosecute identity thieves. The reason, Ms. Wallace explains, is that identity crime often involves small dollar losses for many victims, in some instances, victims are scattered across multiple jurisdictions. This requires a costly investigation that strains the resources of investigators and prosecutors. Ms. Allen indicated that the lack of investigation and prosecution enables large organized identity theft scams to go undetected for months, even years.

Marc Rotenberg noted that identity thieves continue to succeed through phishing, pretexting, spyware, and the mere lack of attention by consumers. This lack of attention, Mr. Rotenberg explained, goes hand in hand with consumers' lack of knowledge regarding the true dangers that may be present. Mr. Rotenberg further noted that users are often focused on their primary tasks and may not notice security indicators or read warning messages that could prevent them from becoming victims of identity theft.

Don Rebovich noted that close to half of the identity theft crimes depended upon offenders working in criminal groups. Dr. Rebovich explained that the more identity theft foot soldiers that "fan out" to open new accounts, purchase new credit cards, and write bad checks, the more profits criminal organizations can divide amongst criminal organization members.

Don Rebovich further indicated that, nationally, local law enforcement is either lacking or requires improvement in 1) formal written policies specific to identity theft response and investigation; 2) follow up contacts of identity theft victims; 3) the provision of copies of the written reports taken by the officers to the reporting victims; 4) utilization of the Federal Trade Commission's (FTC) Identity Theft Affidavit; and 6) an emphasis on the importance of the expression of empathy by police first responder to victims of identity theft.

A current and emerging issue of identity theft noted by Eric Handy was that currently the Master Death Registry does not include the names of all deceased. Mr. Handy explained that identity thieves have been known to scour obituaries, commentaries, and database registries for people who died as children or young adults. Mr. Handy further explained that these individuals then apply for birth certificates and Social Security Number replacement cards to assume that identity. These documents have been known to be reproduced many times and sold to multiple people. This crime, Mr. Handy noted, may go unnoticed for months, even years, until families of the deceased receive calls from collection agencies.

Topic Two: Improvement of Public and Private Assistance Efforts to Victims of Identity Theft

The following were some of the recommendations made by individuals in the second panel, in their written testimonies, on how public and private assistance efforts to victims of identity theft can be improved:

Catherine Allen pointed out that thus far only 44 states have created laws requiring organizations notify every person whose privacy was compromised due to employee lost or leaked data. Ms. Allen recommended the remaining states implement similar laws to prevent organizations from placing customers' privacy at risk.

Mark Rotenberg recommended the Department of Homeland Security and the Office of Science and technology to stop the commercialization of personal data held by government agencies as well as to apply the Privacy Act to all data collected by the government and government contractors.

Don Rebovich recommended actions should be taken to expunge identity theft victim names and information from criminal justice databases to prevent victims from being falsely arrested for crimes committed by identity thieves.

Dr. Rebovich also recommended that managers in the public and private sectors implement methods to prevent employees from misusing customer's information. Some preventative methods mentioned by Dr. Rebovich include: 1) effective employee screening methods at hiring; 2) effective monitoring/surveillance of employee activities in both the real and virtual settings; 3) limitation of data access to only select employees; and 4) the establishment of public notification of employer policies on employee interaction with data and the repercussions/penalties for violations.

Don Rebovich further recommended to not overlook the importance of educating the public on the finer points of doing everything one can to prevent identity victimization to begin with. Dr. Rebovich noted that experts in identity theft prevention have point out simple practices that can be followed to dramatically reduce the risk of becoming an identity theft victim. Some of these practices noted by Dr. Rebovich include: 1) safeguarding social security numbers; 2) minimizing the amount of personal information one carries; 3) reducing the sharing of personal information and being alert to credit card skimming tactics. Other practices pointed out by Dr. Rebovich include simple computer use practices such as enabling strong password protection, encrypting files, and being alert to common phishing and related scams. Dr. Rebovich further noted that the general public should understand actions that can be taken to limit the extent of identity theft

victimization. This can be done through the early recognition of identity theft by practicing the routine review of: personal credit report, monthly financial statements, and social security earning and benefits statements.

Anne Wallace pointed out that ITAC sends information concerning identity theft incidents to the U. S. Postal Inspection Service's Financial Crime Database to be used by postal inspectors all over the country. ITAC, Ms. Wallace indicted, also shares this information with the Federal Trade Commission's Consumer Sentinel Database. This is a database used by approximately 1,400 local, state, and federal agencies, including the FBI and the Secret Service.

Eric Handy recommended the creation of a database that contains the name, month, year of birth, and Social Security Number of every individual from the age of 1 day to 17 years and 10 months. This information, Mr. Handy noted, should be shared with credit reporting agencies, all Departments of Motor Vehicles, and selected companies performing credit application prescreening to prevent identity thieves from misusing identities of individuals under the age of 18.

Mr. Handy also recommended all government agencies that issue death certificates to notify within 10 business days of the issuance of a death certificate, the death of an individual to the Office of Social Security Administration. The notification, Mr. Handy recommended, could be done either by certified mail or through a certified online form. The Social Security Administration should, in turn, notify all credit reporting agencies/repositories within 15 business days that an individual's SSN be flagged. The credit reporting agencies, Mr. Handy recommended, should in turn enter a "deceased alert statement" in the deceased's credit report declaring: *This person died on (date). New credit lines should not be extended to this name and/or social security number from that date forward.*

Topic Three: Methods to Increase prosecution and Deterrence of Identity Thieves

The following were some of the recommendations made by members of the second panel, in their written testimony, on how to increase prosecution and deterrence of identity thieves:

Catherine Allen pointed out that the enactment of the Identity Theft Enforcement and Restitution Act of 2008 has made it possible to bring felony charges against multiple offenders. The Act, Ms. Allen noted, also allows crimes committed within a single state to be prosecuted in federal courts, and directs the U.S. Sentencing Commission to review its guidelines to consider increasing the penalties for those convicted of identity theft, computer fraud, illegal wiretapping, or breaking into computer systems. Anne Wallace similarly recommended the implementations of stiffer sentences for identity theft criminals.

Don Rebovich underscored the importance of research studies that recommend government should infuse resources into "best practices" training programs designed to build upon lessons learned from effective federal, state, and local law enforcement strategies. According to Dr. Rebovich, these programs should be directed nationally to local law enforcement officers to effectively identify and investigate identity theft crimes.

Dr. Rebovich also recommended the support of prosecutorial associations like the National Association of District Attorneys (NDAA) and the National Association of Attorneys General

(NAAG) in efforts to emphasize the urgency of the prosecution of identity theft and provide training to enhance prosecutors' abilities to prosecute identity thieves. Anne Wallace similarly recommended the support of initiatives such as the National Computer Forensics Institute in Hoover, Alabama to provide crucial training for law enforcement, prosecutors, and judges.

To read each of the public and private organization's testimonies, access the Congressional Subcommittee's website at http://informationpolicy.oversight.house.gov/ , click on the "Hearings" section. The title of the hearing was *Identity Theft: Victim's Bill of Rights*. To read Dr. Don Rebovich testimony click here to download