Identity Theft:
An Annotated Bibliography of Government Resources

Methodology.

The topic of identity theft is no small issue. With the exponential advent of digital technology, there has been a correlating increase among identity theft occurrences and techniques, and consequently, in government attention. This makes an exhaustive bibliography of the topic improbable, and some editorial measures must be taken. Identity theft can fall anywhere within a large range of criminal activities: check washing, data mining, credit fraud, biometrics, forgery, illegally obtaining, producing, or distributing government identification documents, phishing, ghosting, pretexting, et cet. While all these topics are legitimate aspects of identity theft, I found there is a reasonably digestible amount of information on the topic in general. Though some of the documents referenced herein do have niche focuses, largely they are present because of either their relevance to identity theft as a whole or because they typify a form of resource or research slant.

Also, it should be noted that no "proposed" legislation is included in this bibliography (though some congressional documents related to such do appear). Like many popular topics on Capitol Hill, various identity theft bills are introduced and lost in committee. That should not, however, warrant any researcher ignoring such efforts, as the bills themselves, and the various reports and studies they propagate, are likely as useful as those that were more successful in their purpose. Also, there are innumerable state legislations, which have passed, but are not contained in this bibliography, though many of these documents can be found using the same resources. And finally, this bibliography excludes international issues of identity theft and the myriad of judicial cases which in some way brush up against "identity theft."

In organization, I attempted to arrange the bibliography by format, in order of descending relevancy. First, is "Enacted Legislation," a fairly complete treatment of any laws passed which greatly affect identity theft issues. These are cited according to where they are found in *United States Statutes at Large*, with codification referenced at the end of each annotation. Within each section, the entries are arranged chronologically beginning with the earliest. (Most essential "identity theft" resources have originated in the past fifteen years).

Next, I show two executive orders and their descendant documents, followed by a number of CRS reports, and then, GAO reports. These lists of reports are not exhaustive, but do represent a majority of the information in their formats. They have been selected topically, with my best judgment, reflecting the most vital "identity theft" issues of the current climate and avoiding recovering similar material. Later documents were preferred over those which likely have become somewhat outdated (especially with those concerning digital technology).

After these come various hearings and reports produced by the Senate and House committees which claim the most jurisdiction over "identity theft." This list is by no means exhaustive and should be consulted merely as a sampling of the type of information that these committees produce. Other committees surely affect "identity theft" as well, and many failed bills have produced reports and hearings, which did not ultimately prove as beneficial.

Then, I move on to specific departments and agencies. While only a few have often published documents on "identity theft," some helpful outlier resources are included to

show that any section of government could feasibly affect the topic at hand. Some of these resources are departmental websites, which though they contain multiple resources, or "pages," are addressed under a single annotation.

Finally, there is a short section concerning statistical data. Its relative size should not mislead the reader, as many of the other resources listed contain vast amounts of statistical data, but required to be classified elsewhere. In this section, a few resources are listed which provide statistics alone on "identity theft," and most often provide statistics on dozens of other topics, too.

All entries are cited according to the University of Memphis Government Citation Guide, and when applicable SuDocs numbers are included at the end of annotations. Most of these resources are available online, and even when, at times, I discovered the information elsewhere on the Internet, I found it again on GPO Access, and cited it as such, so that the citations are as consistent as possible and they reflect the most reliable URLs.

These documents were retrieved using *United States Statutes at Large*, *CSI Congressional Index*, FedStats.gov, GPO Access, Library of Congress's Thomas, and web browsing of government websites.

Enacted Legislation.

1.) **"Truth in Lending Act of 1968." (P.L. 90-321),** ***United States Statutes at Large*****. 82 Stat. 147.**

> An important Ur-legislation that would begin a national discussion on personal information garnered or shared in financial transactions. This law sought to protect consumers seeking credit by requiring the disclosure of key terms regarding the loans. In many cases, the law also limited customer liability for fraudulent credit card charges to a maximum of $50. (15 U.S.C. § 1601)

2.) **"Fair Credit Reporting Act of 1970." (P.L. 91-508),** ***United States Statutes at Large*****. 84 Stat. 1128.**

> The first federal legislation regarding consumer reporting agencies. This law, for the first time, established consumer credit rights in the United States. The FCRA required CRAs to allow the consumer access to the information about him or her in the agency's files and to verify or dispute the information. If negative information was removed by the agency due to a consumer dispute, the FCRA requires that the consumer must be notified before it can be reinstated. Also, the FCRA enacted limitations on how long an agency could retain negative information about a consumer, applying mostly to bankruptcies or tax liens. This act has been greatly amended since 1970. The Consumer Credit Reporting Reform Act of 1996 allowed companies to share information among their affiliates as long as the fact of possible sharing has been clearly notified of the possibility and has an opportunity to opt out.

This later amendment and corporations' interpretation of its rules has caused much controversy. (15 U.S.C. § 1681)

3.) "Privacy Act of 1971." (P.L. 93-579), ***United States Statutes at Large*****. 88 Stat. 1896.**

The purpose of this act was to give citizens greater control over personal identifying information collected and used by the government. An agency may only collect what is "relevant and necessary" for it to meet its functions. Disclosure was also addressed. Though no language in the law addresses any private institutions, the Privacy Act limits how the government may disclose any personal information, requiring written consent from the citizen and a court order (with a list of exceptions). Under this law, any federal, state, or local government agency must communicate if the number is needed, what will be done with it, and what consequences may come from refusing to disclose it.
(5 U.S.C. § 552a)

4.) "Fair Credit Billing Act of 1974." (P.L. 93-495), ***United States Statutes at Large*****. 88 Stat. 1511.**

Enacted as an amendment to the "Truth in Lending Act." This law, for the first time, provides steps for a consumer to take in the case of identity theft. If reported within sixty days of the statement date, a consumer may challenge billing errors due to charges in the wrong amount, goods not received, calculation errors, or, most importantly, charges not made by the consumer. (15 U.S.C. § 1666)

5.) "Electronic Fund Transfer Act of 1978." (P.L. 95-630), ***United States Statutes at Large*****. 92 Stat. 3728.**

The Electronic Fund Transfer Act explicitly outlines rights and responsibilities of any party involved in electronic fund transfers. Some older protections for consumers were transferred from non-electronic fund transfer legislation, while newer steps were made towards consumers' rights. For example: the loss or theft of a credit card, if reported within two business days, would only put the customer at risk for a loss of $50. If not notified by this time, the card-owner can be held accountable for up to $500, and if not reported in 60 days, all funds and fees may be required. (15 U.S.C. § 1693)

6.) "False Identification Crime Control Act of 1982." (P.L. 97-398), ***United States Statutes at Large*****. 96 Stat. 2009.**

This law sought to address fraudulent fabrication and use of personal identification documents. The act included this type of identity theft with

other statutes, making the act federally punishable. Included is language forbidding mailing any private identification documents without a disclaimer. Also, the production, transference, or possession of a "document-making device" with the intent to forge personal documents is punishable by fines and/or imprisonment. (18 U.S.C. § 1028 and 1738)

7.) **"Drivers Privacy Protection Act of 1994." (P.L. 103-322),** ***United States Statutes at Large*****. 108 Stat. 2099.**

This act passed as an amendment to H.R. 3355 (the Omnibus Crime Act of 1994). Until this law passed, anyone was able to access DMV records for any individual at the price of a few dollars. This included address, date of birth, license number, and the individual's full name. Though challenged by a South Carolina court (on the grounds of the law violating principles of federalism), the Supreme Court upheld the law's legitimacy on grounds that it fell under "Congress's authority to regulate interstate commerce." (18 U.S.C. § 2721-2725).

8.) **"Health Insurance Portability and Accountability Act of 1996." (P.L. 104-191),** ***United States Statutes at Large*****. 108 Stat. 2099.**

As a part of many Digital Age legislation efforts in the mid-nineties, the HIPAA requires health insurance agencies and healthcare providers to establish and maintain electronic versions of patient records. These records include "individually identifiable health information…created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university." Curators of such records are required to share their privacy policies with the consumer and to obtain consent before sharing any identifiable health information. Effectually, this means that the consumer must be informed of any security breach in the system. (42 U.S.C. § 1320)

9.) **"Identity Theft and Assumption Deterrence Act of 1998." (P.L. 105-318),** ***United States Statutes at Large*****. 112 Stat. 3007.**

A landmark piece of legislation in regards to identity theft, ITAD is the first enacted law to wholly address the issue. The act established the Federal Trade Commission in order to process and catalog complaints of identity theft victims, as well as inform them on protection measures and what corrective measures may be taken to stem or reverse the consequences of identity theft. Identity theft is, at last, made a federal crime, allowing law enforcement agencies to prosecute with greater ease. Explicit definitions of 'personally identifiable information' are finally given, including a person's name, date of birth, driver's license number, passport number, tax identification number, or alien registration number. (18 U.S.C. § 1028)

10.)"Gramm-Leach Bliley Act of 1999." (P.L. 106-102), ***United States Statutes at Large*****. 113 Stat. 1338.**

Also known as the Financial Services Modernization Act, the GLBA begins to partially provide protection against the sale of consumer financial information. Various agencies are instructed to administer and enforce new regulations on financial privacy by implementing new procedures and policies. The act illegalizes obtaining financial information under false pretenses, whether from the consumer or a financial organization. (15 U.S.C. § 6801)

11.) "Social Security Number Confidentiality Act of 2000." (P.L. 106-433). ***United States Statutes at Large*****. 114 Stat. 1910.**

A small, but important law, which prohibits the display of social security numbers on unopened checks or any Treasury-issued documents. (31 U.S.C. § 3327)

12.)"Internet False Identification Act of 2000." (P.L. 106-578). ***United States Statues at Large*****. 114 Stat. 3075.**

Enacted as an amendment to the False Identification Crime Control Act of 1982, this law aimed to extend provisions and protections from the earlier bill into identity theft issues regarding the Internet. Now, physical possession of a fraudulent personal identification document is no longer necessary for prosecution, as document transfers by electronic means are included as well. Apparently, over the Internet, many were selling fake social security cards under the pretense that they were merely "novelties." (18 U.S.C. § 1001 and 1028)

13.) "The Fair and Accurate Credit Transactions Act of 2003." (P.L. 108-159). ***United States Statutes at Large*****. 117 Stat. 1952.**

FACTA was a large piece of legislation encompassing many different aspects of credit exchanges. Section 5 explicitly references identity theft. Under FACTA, any consumer could request a credit bureau to truncate his or her social security number on a credit report. The act also required many merchants to truncate or blur parts of credit card numbers on receipts and order forms. A victim of identity theft is now enabled to work with creditors on removing negative information from their credit report. This law also gives every citizen the right to order a copy of their credit report once every year without paying any fee. Three "alert" systems are established to prevent identity theft. If a consumer feels that they may have been or soon will be an identity theft victim, they may place an "initial alert" on their file. If they have recently been declared a victim, they may have an "extended alert," and military officials are able to place an "active duty alert" on their files when

they are away from their usual post. These alerts place the consumer's files under greater scrutiny and limit how a credit agency may share or sell information to affiliate organizations. (U.S.C. § 1681)

14.) **"Identity Theft Penalty Enhancement Act of 2004." (P.L. 108-275).** ***United States Statutes at Large*****. 118 Stat. 831.**

In attempts to place greater deterrence on professional identity thieves, this law increases penalties and creates a new term for continuous or egregious offenders. "Aggravated identity theft" refers to theft in which the information stolen is used to commit even greater crimes, such as illegal acquisition of firearms, immigration violations, and terrorist acts. Also, those who commit identity theft at their place of work now face greater penalties. (18 U.S.C. § 1028A)

15.) **"Telephone Records and Privacy Protection Act of 2006." (P.L. 109-476).** ***United States Statutes at Large*****. 120 Stat. 3568.**

Building upon some aspects of the Gramm-Leach-Bliley Act, this law further illegalizes the act of "pretexting." Pretexting involves obtaining information illegally through various forms of pretense and fraudulent tactics, specifically those methods which require someone assuming a false identity or researching a person or company beforehand, in order to acquire private information more easily. The maximum penalty for pretexting under this act is 10 years in federal prison. Specifically, the act was drafted to stem the large number of pretexting incidents involving personal phone records.

Executive Actions

1.) **"Strengthening Federal Efforts to Protect Against Identity Theft." E.O. 13402. 71** ***Federal Register*** **(10 May 2006). ONLINE. Available: http://edocket.access.gpo.gov/2006/pdf/06-4552.pdf [19 April 2010].**

a. **"Amendment to Executive Order 13402, Strengthening Federal Efforts to Protect Against Identity Theft." E.O. 13414. 71** ***Federal Register*** **(8 November 2006). ONLINE. Available: http://edocket.access.gpo.gov/2006/pdf/06-9148.pdf [19 April 2010].**

E.O. 13402 was signed by George W. Bush in order to increase efforts in prosecuting identity thieves. This was warranted by an exponential growth in number of identity theft cases since 2000 (likely due to the ever-growing presence of the Internet). The order sought to increase "aggressive law enforcement actions," improve public outreach to educate about identity theft, and increase safeguards within Federal departments and agencies to better protect personal data held by the government. Also, this order established the Identity Theft Task Force in order to research data and formulate ideas on how best to implement these initiatives. E.O. 13414

extends the date by which this task force should report back to the president to February 9, 2007, though it also includes provisions to miss this deadline as well.

2.) **U.S. Department of Justice. President's Identity Theft Task Force. *Summary of Interim Recommendations*. ONLINE. Federal Trade Commission. September 2006. Available: http://www.ftc.gov/os/2006/09/060916interimrecommend.pdf [19 April 2010].**

Until the presidential task force could complete their entire report, they offered to the president some recommendations on measures that could be taken immediately to begin governmental reform regarding identity theft. These included: 1.) Distributing guidance sheets to all federal agencies which outlined how to prevent identity theft and procedures in the case of a security breach, 2.) Requesting the OMB and the Department of Homeland Security to produce a list of "best practices" and "common mistakes" regarding identity theft, 3.) Limiting public sector use of SSN's, 4.) Organize a workshop of how to more effectively screen a person's identity, 5.) Allow victims to recover for the value of time spent attempting to remediate identity theft harm, 6.) Allow victims to obtain police reports regarding their identity theft, 7.) Establishing a data breach policy for the public sector, and others.

3.) **U.S. Department of Justice. President's Identity Theft Task Force. *Combating identity theft: A strategic plan*. Washington: Government Printing Office, 2007. (J 1.2:ID 2/2).**

The final and exhaustive report produced by the president's task force. Over a hundred pages, this report provides a glossary of terms and acronyms, a profile of identity thieves and their methods, and a detailed strategy for identity theft prevention. For the most part, the strategy involves the same recommendations as the interim report (above) laid out; however to a much more detailed extent. Greater attention is paid to law enforcement techniques, more aggressive penalties, and victim recovery.

4.) **www.idtheft.gov**

The official site of the presidential task force. The home page lays out the task force's purpose, basic strategy, and history of action. One can access the full strategic plan, the interim recommendations, a "fact sheet" on identity theft, the executive orders, and public comments submitted in response to the full report. Also included are two links to the Federal Trade Commission's website on identity theft (below), specifically to the pages regarding victims' rights and how to report an identity theft.

CRS Reports

1.) **U.S. Library of Congress. Congressional Research Service.** ***Identity Theft and the Fair Credit Reporting Act: An Analysis of TRV v. Andrews and Current Legislation*** **by Angie A. Welborn. ONLINE. September 2003. Available: http://assets.opencrs.com/rpts/RS21083_20040105.pdf [15 April 2010].**

Under the Fair Credit Reporting Act, a victim of identity theft can file suit to recover financial losses. However, a two-year statute of limitations is imposed. The Supreme Court oversaw a case on November 13, 2001 in attempts to interpret when this statute of limitations began to run. The Court ruled that the statue of limitations begins at the first instance of inaccurate spending and not when the consumer first learns about the inaccuracies. This report includes a summary of the Fair Credit Reporting Act aspects which are applicable, an analysis of the case, and an analysis of proposed legislation in the wake of the decision. (CRS-RS21083)

2.) **U.S. Library of Congress. Congressional Research Service.** ***Identity Theft: The Internet Connection*** **by Marcia S. Smith. ONLINE. March 2005. Available: http://fpc.state.gov/documents/organization/45263.pdf [15 April 2010].**

Growing instances of Internet-related identity theft prompted Congress to investigate the Web's role in the criminal industry as a whole. Certain high-profile incidences regarding large corporations, such as Bank of America, ChoicePoint, and Lexis Nexis, where over a million Americans became the victims of identity theft, have rekindled interest in further legislation. This report examines those occurrences, compares Internet and non-Internet cases of identity theft, and explores the Web-specific method of "phishing." (CRS-RS22082)

3.) **U.S. Library of Congress. Congressional Research Service.** ***Personal Data Security Breaches: Context and Incident Summaries*** **by Rita Tehan. ONLINE. May 2007. Available: http://assets.opencrs.com/rpts/RL33199_20070507.pdf [15 April 2010].**

An extension to the above document, this report continues to investigate security breaches a major financial services firms and data brokers. Since the publication of the earlier report, multiple measures have been introduced into Congress, but none have yet been enacted. (CRS-RL33199)

4.) **U.S. Library of Congress. Congressional Research Service.** ***The Internal Revenue Service's Private Tax Debt Collection Initiative: Current Status, Legislative Proposals, and Issues for Congress*** **by Gary Guenther. ONLINE. September 2008. Available: http://assets.opencrs.com/rpts/RL33231_20080923.pdf [15 April 2010].**

The American Jobs Creation Act of 2004 allowed the Internal Revenue Service to make use of private debt collection agencies in order to more efficiently collect overdue taxes of individuals. An aggressive policy set in place hopes to earn almost three billion dollars by the year 2016. Though the IRS predicts greater efficiency and fairer tax standards through this plan, many critics argue that trained IRS agents should handle the information and not employees of the private agencies. This report explores legal implications and policy issues. (CRS-RL33231)

Government Accountability Office Reports

1.) **U.S. Government Accountability Office.** ***Social Security Numbers: Governments could do more to reduce display in public records and on identity and on identity cards: report to Chairman, Subcommittee on Social Security, Committee on Ways and Means, House of Representatives.*** **ONLINE. GPO Access. November 2004. Available: http://purl.access.gpo.gov/GPO/LPS55812 [8 April 2010].**

Social Security numbers are used widely throughout the public and private sectors. They also are a common target for identity thieves. In recent years, concern has been raised on how visible and accessible citizens' SSNs are in public documents. The GAO examines the extent to which SSNs are visible in records available to the public, the various reasons for the government's collection and display of SSNs, and the formats in which they are stored. (GA 1.13:GAO-05-59)

2.) **U.S. Government Accountability Office.** ***Identity Theft: Some outreach efforts to promote awareness of new consumer rights are under way: report to congressional committees.*** **ONLINE. GPO Access. June 2005. Available: http://purl.access.gpo.gov/GPO/LPS61613 [8 April 2010].**

Composed in response to the Fair and Accurate Credit Transactions (FACT) Act, this report provides information on outreach efforts to inform consumers, business, and law enforcement entities about the law as well as information on the views of relevant groups on the provision's expected impact. Also addressed is the Federal Trade Commission's methodology for constructing its summary of victims' rights and views on the summary's potential usefulness (GA 1.13: GAO-05-710)

3.) **U.S. Government Accountability Office.** ***Personal Information: Key federal privacy laws do not require information resellers to safeguard all sensitive data.*** **ONLINE. GPO Access. June 2006. Available: http://purl.access.gpo.gov/GPO/LPS73295 [8 April 2010].**

Information resellers, companies that collect and resell publicly available and private information on individuals, have brought about greater concerns

about privacy and security. This report examines the use of resellers by financial firms, what laws, if any, are applicable to resellers, any oversight of resellers by federal regulators, and oversight of with financial firms' adherence to data security laws. The report also offers recommendations on these issues. (GA 1.13:GAO-06-674)

4.) **U.S. Government Accountability Office.** ***Tax Administration: Internal Revenue Service has implemented initiatives to prevent, detect, and resolve identity theft related problem, but needs to assess their effectiveness: report to congressional requesters*****. ONLINE. GPO Access. September 2009. Available: http://purl.access.gpo.gov/GPO/LPS117552 [8 April 2010].**

The Internal Revenue Service often becomes a secondary victim to identity theft. When thieves use a taxpayer's name or SSN to fraudulently claim a refund or to gain employment, the IRS receives duplicate claim forms or discovers unreported wages and, then, must expend great effort and resources in rectifying the issue. This report describes the extent of identity theft related refund and employment fraud and assesses the IRS's initiatives thus far to prevent and resolve such problems. The GAO also investigates the state and possible future of interagency cooperation on such issues. (GA 1. 13:GAO-09-882)

Congressional Committees Reports and Hearings

House Energy and Commerce Committee

1.) **U. S. House. Committee on Energy and Commerce. Subcommittee on Commerce, Trade, and Consumer Protection.** ***Data Security: the discussion draft of data protection legislation*** **Hearing, 28 July 2005. ONLINE. GPO Access. July 2005. Available: http://purl.access.gpo.gov/GPO/LPS73895 [12 April, 2010].**

In order to better understand the issues of data security, this hearing was held so that committee members may hear about the issues from experts in the field. Testimonies include high-ranking officials in Entrust, Inc., Microsoft Corp., Electronic Privacy Information center, and TRUSTe. This is an excellent resource for raw experiences not yet edited by committee reports or legislation. (Y 4.C-73/8:109-48)

2.) **U.S. House. Committee on Energy and Commerce. Subcommittee on Commerce, Trade, and Consumer Protection.** ***Social security numbers in commerce: Reconciling beneficial uses with threats to privacy*** **Hearing, 11 May 2006. ONLINE. GPO Access. May 2006. Available: http://purl.access.gpo.gov/GPO/LPS73895 [12 April, 2010].**

With much discussion in data security being focused on the use, dissemination, and protection of SSN's, this hearing includes testimony of both CEOs of relevant companies (Electronic Privacy Information Center, Pension Benefit Information, Morrison & Foester, LLP) and government officials, such as Jon Leibowitz, commissioner of the FTC and Lauren Steinfeld from the Office of Management and Budget. (Y 4.C 73/8:109-91)

3.) **U.S House. Committee on Energy and Commerce. Subcommittee on Commerce, Trade, and Consumer Protection. *Combating spyware: H.R. 964, the Spy Act* Hearing, 15 March 2007. Washington: Government Printing Office, 2008.**

The Internet has brought about many ingenious and insidious new methods of identity theft, so many that the federal government has had a difficult time keeping up. Spyware is one of the most widely used Web techniques. This hearing was convened in support of H.R. 964, "The Spy Act," which hopes "to protect users of the Internet from unknowing transmission of their personally identifiable information through spyware programs, and for other purpose." Witnesses include various executive members of Web-based corporations, who share their experience and insight on spyware and how it works. (Y 4.C73/8:110-21)

House Judiciary Committee

1.) **U.S. House. Committee on the Judiciary. Subcommittee on Crime, Terrorism and Homeland Security. *Cyber-Security Enhancement and Consumer Data Protection Act of 2006* Hearing, 11 May 2006. ONLINE. GPO Access. May 2006. Available: http://purl.access.gpo.gov/GPO/LPS73380 [11 April 2010].**

In order to better inform the Consumer Data Protection Act, a hearing was held. The hearing attempted to address how deter past crimes from being repeated and prevent future techniques from being developed. Also, the hearing hoped to garner suggestions from witnesses on how to better protect personally identifiable information and to aggregate resources to provide the Department of Justice. Witnesses were not only interviewed, but offered prepared statements as well. (Y 4.J 89/1:109-106)

2.) **U.S. House. Committee on the Judiciary. Subcommittee on Crime, Terrorism, and Homeland Security. *Privacy and Cybercrime Enforcement Act of 2007* Hearing, 18 December 2007. Washington: Government Printing Office, 2008.**

A further permutation of the above legislation, this hearing further addresses the transition from traditional identity fraud into the digital age. The bill in question seeks to allocate funds for State programs to enforce prosecution of cybercrimes. This legislation also aims to allow identity theft victims to seek restitution for loss of time and money spent restoring their credit, whereas

prior, one could only recuperate direct financial loss. Discussion includes these topics and, also, debate over how best to prosecute identity theft consistently, so as to provide effective deterrents towards cybercriminals. (Y 4.J 89/1:110-128)

Senate Commerce Committee

1.) **U.S. Senate. Committee on Commerce, Science and Transportation.** ***Identity Theft Prevention Act of 2007: report of the Committee on Commerce, Science, and Transportation on S.1178.*** **(S. Rpt. 110-235) ONLINE. GPO Access. December 2007. Available: http://purl.access.gpo.gov/GPO/LPS88654 [18 April 2010].**

The bill S. 1178 is an attempt to strengthen data protection and safeguards, require data breach notification, and further prevent identity theft. This committee report provides background information, requests further resources, proposes amendments, and ultimately passes the bill to move to the floor for a vote. This bill would allow consumers to freeze their credit reports at will. Also notable, it would require financial firms' to more thoroughly check the credentials of any third-party organizations that they share their information with regularly. (Y 1.1/5:110-235)

Senate Judiciary Committee

1.) **U.S. Senate. Committee on the Judiciary. Subcommittee on Terrorism, Technology and Homeland Security.** ***Securing electronic personal data: Striking a balance between privacy and commercial and governmental use*** **Hearing, 13 April 2005. Washington: Government Printing Office, 2005.**

This hearing is invaluable to the study of identity theft because it deals with the topic so broadly and efficiently. The electronic storage of vast amounts of personal data that recent years has brought about is shown to be both necessary and dangerous. Ten witnesses testify to the respective views of data storage of the individual, the corporation, and the government. (Y 4.J 89/2:s.HRG.109-60)

2.) **U.S. Senate. Committee on the Judiciary.** ***Personal Data Privacy and Security Act of 2009: report (to accompany S. 1490) (including cost estimate of the CBO).*** **(S. Rpt. 111-110). Washington: Government Printing Office, 2009.**

The Personal Data Privacy and Security Act of 2009 (S. 1490) seeks to "prevent and mitigate identity theft, to ensure privacy, to provide security protections for personal data, to enhance criminal penalties and law enforcement assistance." This report includes a thorough history of this bill in relation to all other similar legislation that has been proposed before it.

The CBO estimate provides an intriguing insight to the mechanics of how identity theft legislation plays out. Also, the section-by-section summary of the bill both elaborates on the law and simplifies the legalese. (Y 1.1./5:111-110)

Departmental/Agencies Websites

Federal Trade Commission

1.) **www.ftc.gov/identitytheft**

The Federal Trade Commission was created in response to the 1998 legislation regarding identity theft, and by far, it is the most prolific government agency on the topic. The site splits its strategy into the alliterative message of "Deter, Detect, and Defend," with a separate tab for each consumers, businesses, and law enforcement to show how to achieve each goal. A "Media" section shows testimonial videos as well as press releases. However, the most substantial area of the site is the "Reference Desk," which includes links to National Data, State Data, an archive of FTC reports and testimonies reaching back to the agency's inception, a summary of identity theft-related laws, FTC rulemakings, and information on how an organization could partner with the FTC in an awareness campaign, or receive materials to share.

2.) **Federal Trade Commission.** ***National and state trends in fraud and identity theft: January-December 2002*****. ONLINE. GPO Access. August 2003. Available: http://purl.access.gpo.gov/GPO/LPS34403 [17 April 2010].**

This article of almost seventy pages is packed with information. Statistical data sets and infographics abound. The study takes its information gathered from the FTC's Consumer Sentinel, a program for processing identity theft complaints. The raw data has been analyzed and presented in relation to different trends, in order to show how identity theft most often plays out in actual scenarios. The article lists top complaint categories, fraud complaint trends, internet-related trends, trends for identity theft records, complaints by state and age, and how different types of victims go about contacting law enforcement. (FT 1.2:F 86)

3.) **Anderson, Keith B. Federal Trade Commission.** ***Identity Theft: Does the risk vary with demographics?*** **ONLINE. GPO Access. August 2005. Available: http://purl.access.gpo.gov/GPO/LPS79066 [17 April 2010].**

One of the more interesting identity theft resources, this thesis-length study attempts to address identity theft beyond immediate pragmatic measures by investigating the socioeconomic factors involved. In short, the paper examines the likelihood that an individual will experience identity theft due to demographic characteristics. Some conclusions are that women, consumers

with higher income levels, higher education, and those who are the only adult in the household are more likely to become victims. (FT 1.37/2:279)

4.) **Federal Trade Commission.** ***ID Theft: What it's all about.*** **ONLINE. GPO Access. June 2005. Available: http://purl.access.gpo.gov/GPO/LPS104878 [17 April 2010].**

A pamphlet printed and distributed by the Federal Trade Commission to raise awareness on identity theft issues. Written plainly and briefly, the brochure explains how identity theft occurs, how to tell if you are a victim, how to get the free annual credit report, how to manage personal information, fraud alerts, theft reports, and immediate steps to take if you are an identity theft victim. (FT 1.2:ID 2/4)

5.) **Federal Trade Commission.** ***Business must provide victims and law enforcement with transaction records relating to identity theft*****. ONLINE. GPO Access. May 2006. Available: http://purl.access.gpo.gov/GPO/LPS104051 [17 April 2010].**

This document is a helpful public awareness tool offered up to business curious about how to deal with identity theft issues. It lays out in plain terms what is required from a business under the Fair Credit Reporting Act and how to implement the standards into daily practice. It addresses who must comply to the new regulations, what documents are required for a business to provide, when it is appropriate not to provide documents, where to find more information from the FTC, and how to share comments or suggestions on the law's implementation. (FT 1.33:T 68)

Social Security Administration

1.) **Social Security Administration.** ***Identity theft and your social security number*****. ONLINE. GPO Access. February 2004. Available: http://purl.access.gpo.gov/GPO/LPS57839 [17 April 2010].**

Accessible from www.ssa.gov, this resource consists of a number of electronic leaflets. It is one of the few resources that offers the option of a foreign languages, including Spanish, Arabic, Vietnamese, and Armenian. Mostly geared towards public outreach, the site walks the user through various issues relating to Social Security number theft. After establishing the need and reasons for keeping one's SSN private, the site shows how to tell if someone else is using your SSN and provides clear succinct instructions on how to contact both the SSA and the FTC to have the issue resolved. (SSA 1.19:M 69)

Department of Justice

1.) **www.usdoj.gov**

Though navigating this site's resources and its search engine can be frustrating, it will return unique documents related to identity theft. There is an even mix between documents meant for public awareness and more meaty substance. The COPS (Community Oriented Policing Services) section of the website has compiled a "Guides and Reports," page which abstracts and links to both government and publicly produced material, including the Privacy Rights Clearinghouse, the Identity Theft Resource Center, and the Nathanson Center for the Study of Organized Crime and Corruption, which addresses the issue of transnational crime.

2.) **Department of Justice. *Identity theft*. ONLINE. GPO Access. 2004. Available: http://purl.access.gpo.gov/GPO/LPS106696 [17 April 2010].**

This overview of identity theft provides bulleted information on what constitutes identity theft. A wealth of statistics are available, mostly from the National Crime Victimization Survey, but they are compiled in a singular way, breaking down identity theft by type, specifically separating credit card fraud from the theft of personal information. Victimization is also broken down by households, and the average amount of financial loss is given for each factor. (J 29.42)

3.) **Department of Justice. National Drug Intelligence Center. *Methamphetamine-related identity theft*. ONLINE. GPO Access. May 2007. Available: http://purl.access.gpo.gov/GPO/LPS83680 [18 April 2010].**

A very interesting article with a unique slant. Using data from the Better Business Bureau and the Federal Trade Commission, a correlation is shown between counties and regions with a high level of methamphetamine users and those with high occurrences of identity theft. Southwestern and Western states are most susceptible to drug-related identity theft. While this information may only be situationally useful, it shows how the issue of identity theft has grown beyond simple, pragmatic measures. By using this study as an exemplum, it may be worthwhile to see what other social, cultural, and demographic factors correlate with identity theft criminals and victims alike.(J 1.112:M 56)

Department of Treasury

1.) **Department of the Treasury. "Identity Theft Resource Page." ONLINE. Available: http://www.identitytheft.gov [17 April 2010].**

This rather humble site does contain a few resources that are not present elsewhere. It provides a brief summary of what various government agencies are doing to combat identity theft. It also shows the progress of many of the

presidential task force recommendations as well as a webcast of the task force press conference.

2.) **Department of the Treasury. *Security awareness and identity theft*. ONLINE. March 2006. Available: http://purl.access.gpo.gov/GPO/LPS78054 [17 April 2010].**

A public awareness publication produced by the IRS. This brochure highlights simple prevention methods to avoid identity theft, tips on how to judge whether or not a request for information is legitimate, and how a citizen may acquire his or her free annual credit report. Also included are various government hotlines and resources if one feels they may have become victim to identity theft. (T 22.44/2:4524)

Postal Inspection Service

1.) **www.postalinspectors.uspis.gov**

This website outlines the United States Postal Service's policies and procedures regarding identity theft. This includes regulations on how one can protect one's identity when mailing letters or packages, explanations of how postal inspectors prevent and discover identity theft through their inspections, and frequently asked questions about how to better protect personally identifiable information. This could be a valuable niche resource in comparing interagency policies.

Federal Deposit Insurance Corporation

1.) **http://www.fdic.gov/consumers/consumer/alerts/theft.html**

This single page amongst the FDIC's entire webpage compiles all of its resources about identity theft. Though not updated since May 2009, a variety of resources are still available, well-organized with working links. They include Financial Institution Letters, consumer alerts, public awareness brochures, press releases, a couple of FDIC studies, consumer news articles, and even some humorous videos to help explain practical and useful messages about "phishing."

Statistics

1.) **Bureau of Justice Statistics (http://bjs.ojp.usdoj.gov)**

This resource provides a wealth of statistical data on almost any topic. In terms of identity theft, most data is extracted and formulated into tables based on the National Crime Victimization Survey. Most data sets are constructed for the purpose of expressing demographic and frequency statistics about identity theft victimization and its consequences, both in

objective terms and subjective testimonies Another interesting table shows how the vast number of identity theft cases, though felony charges, are tried in State courts by State prosecutors. Methodology concerning the NCVS can be found here, as well.

2.) **U.S. Census Bureau. Statistical Research Division.** ***Final Report of Cognitive Research on the New Identity Theft Questions for the 2004 National Crime Victimization Survey*** **by Kristen Hughes. ONLINE. August 2004. Available: http://www.census.gov/srd/www/abstract/ssm2004-02.html [19 April 2010].**

In response to changes in the National Crime Victimization Survey, this report analyzes how data collection is keeping up with the changing climate of identity theft. Constructive criticisms of method, language, and response as well as analysis of the 2004 answers show how different iterations of identity theft affect people in various ways. Also, a healthy amount of attention is given to extracting from interviewees a sense of public knowledge about identity theft.

3.) ***Statistical Abstract of the United States 2010*****. "Table 309: Fraud and Identity Theft – Consumer Complaints by State." ONLINE. 2010. Available: http://www.census.gov/compendia/statab/2010/tables/10s0309.pdf [19 April 2010].**

Merely one example of many useful statistics available through the *Statistical Abstract*… This graph usefully breaks down U.S. fraud complaints and identity theft victims in number and rate by state. This provides a geographical index, which, if in combination with other data, could show how, where, and why identity thieves strike where they do.

Non-Government Web Resources

1.) CDIA Fact Center (http://www.consumerdatareporting.org/ShowPage.aspx?page=identity-theft)
2.) National Institute of Justice. "Identity Theft: A Research Review." (http://www.ojp.usdoj.gov/nij/publications/id-theft/welcome.htm)
3.) AARP (www.aarp.org)
4.) Better Business Bureau (www.bbb.org)
5.) Privacy Rights Clearinghouse (www.privacyrights.org)
6.) National Consumers League (www.nclnet.org)
7.) National Criminal Justice Reference Service (www.ncjrs.org)
8.) Credit Union National Association (www.cuna.org)
9.) Identity Theft Resource Center (www.idtheftcenter.org)
10.) American Bankers Association(www.aba.com)