Order Code RL34028

CRS Report for Congress

Identity Theft Laws: State Penalties and Remedies and Pending Federal Bills

Updated August 6, 2007

Tara Alexandra Rainson
Law Librarian
Knowledge Services Group

Prepared for Members and
Committees of Congress

Identity Theft Laws: State Penalties and Remedies and Pending Federal Bills

Summary

This report provides an overview of state laws on identity theft. It discusses state laws that penalize identity theft, as well as state laws that assist identity theft victims, including those that permit consumers to block unauthorized persons from obtaining their credit information, known as "security freezes." The report also includes a survey of state "credit freeze" statutes. The report concludes with summaries of federal identity theft legislation pending in the 110th Congress.

The report will be updated as warranted.

Contents

List of Tables

Identity Theft Laws: State Penalties and Remedies and Pending Federal Bills

Introduction

This report provides an overview of state laws on identity theft.[1] Fifty states and the District of Columbia have criminal identity theft statutes.[2] Many of these include both monetary penalties and imprisonment. For example, in California imposters are subject to a fine and confinement in jail for up to one year.[3] In Louisiana, imposters are subject to a fine of up to $10,000 and confinement in jail for up to 10 years.[4] Several state statutes include restitution provisions. In Texas, Virginia, and Maryland, the court may order the imposter to reimburse the victim for expenses incurred because of the theft, such as lost income or expenses associated with correcting an inaccurate credit report.[5] Other states impose civil penalties for identity theft activities and provide victims with judicial recourse for damages incurred as a result of the theft. In Washington, imposters are liable for civil damages of $1,000 or actual damages, whichever is greater.[6] The definition of identity theft varies across state codes. Idaho, for example, simply criminalizes the use of "identifying

---

[1] For further information, see *New Data Security Laws Take Effect in Several States*, 75 U.S.L.W. 25 (2007); Emily Farr, *Identity Theft: Liability for Furnishers of Credit Information*, 17 S.C. Law. 42 (2006); Sean C. Honeywill, *Data Security and Data Breach Notification for Financial Institutions*, 10 N.C. Banking Inst. 269 (2006); Kasim Razvi, *To What Extent Should State Legislatures Regulate Business Practices as a Means of Preventing Identity Theft?*, 15 Alb. L.J. Sci. & Tech. 639 (2005); Lilia Rode, *Database Security Breach Notification Statutes: Does Placing the Responsibility on the True Victim Increase Data Security?*, 43 Hous. L. Rev. 1597 (2007); Paul M. Schwartz and Edward J. Janger, *Notification of Database Security Breaches*, 105 Mich. L. Rev. 913 (2007); Kenneth M. Siegel, *Protecting the Most Valuable Corporate Asset: Electronic Data, Identity Theft, Personal Information, and the Role of Data Security in the Information Age*, 111 Penn St. L. Rev. 779 (2007); Gary M. Victor, *Identity Theft, Its Environment and Proposals for Change*, 18 Loy. Consumer L. Rev. 273 (2006); Kamaal Zaidi, *Identity Theft and Consumer Protection: Finding Sensible Approaches to Safeguard Personal Data in the United States and Canada*, 19 Loy. Consumer L. Rev. 99 (2007).

[2] For a complete list of state criminal identity theft statutes, see [http://www.ftc.gov/bcp/edu/microsites/idtheft/reference-desk/state-criminal-law.html].

[3] Cal. Penal Code §§ 530.5-530.7.

[4] La. Rev. Stat. Ann. § 14:67.16.

[5] Tex. Penal Code § 32.51; Va. Code Ann. §§ 18.2-186.3 - 18.2-186.5; Md. Crim. Law Code Ann. § 8-301.

[6] Rev. Code Wash. § 9.35.020(3).

information."[7] In Oregon and Maine, criminal identity theft includes fraudulent use of credit cards.[8] Massachusetts and Illinois criminalize fraudulent credit card use, but also specifically address the fraudulent use of a credit card number or other identifying number.[9]

State "Credit Freeze" Laws[10]

Thirty-seven states and the District of Columbia currently have "security freeze" laws (also "credit freeze" laws) as a form of identity theft victim assistance.[11] A security freeze law allows a consumer to block unauthorized third parties from obtaining his or her credit report or score. A consumer who places a security freeze on his or her credit report or score receives a personal identification number to gain access to credit information or to authorize the dissemination of credit information. A survey of these laws is provided in **Table 1**.

Benefits of security freeze laws include increased consumer control over access to personal information and corresponding decreased opportunities for imposters to obtain access to credit information. Critics of security freeze laws argue that security freezes may cause consumers unwanted delays when they must provide third party institutions access to credit histories for such purposes as qualifying for loans, applying for rental property leases, and obtaining mortgage rate approval.[12] In an

---

[7] Idaho Code Ann. § 18-3126.

[8] Ore. Rev. Stat. § 165.055; Me. Rev. Stat. Ann. tit. 17-A, § 905-A.

[9] Mass. Gen. Laws ch. 266, § 37E; 720 Ill. Comp. Stat. 5/16G-10.

[10] Pursuant to recent Fair and Accurate Credit Transactions Act (FACT) amendments to the Fair Credit Reporting Act (FCRA), federal law may preempt some state provisions relating to identity theft. P.L. 108-159, 117 Stat. 1952. For effective dates, see 68 Fed. Reg. 74,467 and 68 Fed. Reg.74,529 (December 24, 2003). The preemption of these provisions in state law does not apply to any state law in effect on the date of enactment of the Consumer Credit Reporting Reform Act of 1996. 15 U.S.C. 1681t(b)(1)(E). The FCRA, as amended, includes several provisions aimed at preventing identity theft or assisting victims. These new provisions preempt similar state laws relating to the blocking of information in a consumer's credit report resulting from identity theft,with some exceptions. For more information see CRS Report RS21449, *Fair Credit Reporting Act: Preemption of State Law*, by Margaret Mikyung Lee.

[11] The states with enacted security freeze laws are: Arkansas, California, Colorado, Connecticut, Delaware, District of Columbia, Florida, Hawaii, Illinois, Indiana, Kansas, Kentucky, Louisiana, Maine, Maryland, Minnesota, Mississippi, Montana, Nebraska, Nevada, New Hampshire, New Jersey, New Mexico, New York, North Carolina, North Dakota, Oklahoma, Pennsylvania, Rhode Island, South Dakota, Tennessee, Texas, Utah, Vermont, Washington, West Virginia, Wisconsin, and Wyoming. See *State Security Freeze Laws* [http://www.consumersunion.org/campaigns/learn_more/003484indiv.html].

[12] Statement of Stuart K. Pratt, President and Chief Executive Officer, Consumer Data Industry Association, in Congress, Senate, Hearing Before the Senate Committee on Banking, Housing, and Urban Affairs, *Examining The Financial Services Industry's*

(continued...)

effort to balance these interests of security and accessibility, seven states permit consumers to initiate security freezes only if they have been victims of identity theft or attempted identity theft.[13]

State laws also differ regarding what fees, if any, a credit reporting agency (CRA) may charge consumers for requesting a security freeze. Twenty-six states and the District of Columbia prohibit CRAs from charging fees to an identity theft victim who requests a freeze.[14] For example, the Wisconsin identity theft statute provides that there shall be no fee imposed on an individual who submits "evidence satisfactory to the consumer reporting agencies" that he or she has filed an identity theft report with a law enforcement agency.[15] In Vermont, CRAs may impose a fee when the requester is not an identity theft victim.[16] Under the Kansas identity theft statute, CRAs may not charge a security freeze fee.[17] Most state laws specify the maximum fee a CRA may charge per security freeze request.[18]

In addition to security freeze statutes, five states have enacted "credit information blocking" laws.[19] Alabama, Colorado, Idaho, and Washington require consumer credit reporting agencies to block false information resulting from identity theft from victims' credit reports.[20] California requires a debt collector to stop

---

[12] (...continued)
Responsibilities and Role in Preventing Identity Theft and Protecting the Sensitive Financial Information of Their Customers, hearings, 109th Cong., 1st sess., September 22, 2005, available at [http://banking.senate.gov/_files/pratt.pdf]. Hearing available online at [http://banking.senate.gov/index.cfm?Fuseaction=Hearings.Detail&HearingID=170].

[13] 2007 Ark. Act 391; Haw. Rev. Stat. Ann. §§ 489P-3 - 489P-5; Kan. Stat. Ann. §§ 50-723 - 50-724; 2007 Miss. Laws ch. 585; S.D. Codified Laws § 54-15-1, *et seq.*; Tex. Bus. & Com. Code §§ 20.031-20.04; Wash. Rev. Code §§ 19.182.170 - 19.182-200.

[14] Cal. Civ. Code §§ 1785.11.2-1785.11.6; Colo. Rev. Stat. § 12-14.3-102, *et seq.*; D.C. Code §§ 3861-3864; Fla. Stat. § 501.005; 815 Ill. Comp. Stat. 505/2MM; Ky. Rev. Stat. §§ 367.363 - 367.370; La. Rev. Stat. § 9:3571.1 (H) to (Y); Me. Rev. Stat. Ann. tit. 10 § 1313-C; 2007 Md. Laws Ch. 307; Minn. Stat. § 13C.016; 2007 Mont. Laws ch. 138; Nebraska, 2007 Leg. Bill 674; Nev. Rev. Stat. § 598C.010, *et seq.*; Rev. Stat. N.H. §§ 359-B:22 *et seq.*; 2007 N.M. Laws ch. 106; N.Y. Gen. Bus. Law 380-a, *et seq*; N.C. Gen. Stat. § 75-60, *et seq.*; N.D. Cent. Code ch. 51-33; Okla. Stat. tit. 24, § 149, *et seq.*; 2006 Pa. Laws ch. 163; R.I. Gen. Laws § 6-48-1 *et seq.*; 2007 Tenn. Pub. Act ch. 170 (to be codified at Tenn. Code Ann. tit. 46, ch. 18, part 21); Tex. Bus. & Com. Code §§ 20.031-20.04; Utah Code Ann. § 13-42-102 and §§ 13-45-201 - 13-45-205; W. Va. Code § 46A-6L-102; Wis. Stat. § 100.54; Wyo. Stat. §§ 40-12-502 - 40-12-506.

[15] Wis. Stat. § 100.54.

[16] Vt. Stat. Ann. tit. 9, § 2480h.

[17] Kan. Stat. Ann. § 50-723

[18] See, e.g., Cal. Civ. Code § 1785.11.2; Conn. Gen. Stat. § 36a-701a; and D.C. Code § 28-3862, specifying a maximum ten dollar charge.

[19] For further information, see [http://www.ftc.gov/bcp/edu/microsites/idtheft/law-enforcement/credit-info-blocking.html].

[20] Ala. Code § 13A-8-200; Colo. Rev. Stat. §§ 12-14.3-106.5 to 12-14.3-106.9; Idaho Code (continued...)

collection when the alleged debtor provides evidence of his status as an identity theft victim.[21]

Table 1. Survey of State "Security Freeze" Laws

State Security Freeze Statute	Applies to All Consumers?	Credit Reporting Agency Fees for Freeze Requests?	Effective Date
Arkansas, 2007 Ark. Act 391	No. Applies to identity theft victims.	Yes.	Jan. 1, 2008
California, Cal. Civ. Code §§ 1785.11.2-1785.11.6	Yes	Yes. No fee for identity theft victims.	Jan. 1, 2003
Colorado, Colo. Rev. Stat. § 12-14.3-102, *et seq*.	Yes	No fee for first request. No fee for identity theft victims.	July 1, 2006
Connecticut, Conn. Gen. Stat. § 36a-701a	Yes	Yes	Jan. 1, 2006
Delaware, Del. Code Ann. tit. 6, § 2201, *et seq.*	Yes	Yes	Sept. 29, 2006
District of Columbia, D.C. Code §§ 28-3861- 28-3864	Yes	Yes. No fee for identity theft victims.	July 1, 2007
Florida, Fla. Stat. § 501.005	Yes	Yes. No fee for identity theft victims.	July 1, 2006
Hawaii, Haw. Rev. Stat. Ann. §§ 489P-3 - 489P-5	No. Applies only to identity theft victims.	No	Jan. 1, 2007
Illinois, 815 Ill. Comp. Stat. 505/2MM	Yes	Yes. No fee for identity theft victims or seniors 65+ years old.	Jan. 1, 2007
Indiana, 2007 Ind. Legis. Serv. P.L. 104-2007 (S.E.A. 403) (West)	Yes	No	Sept. 1, 2007
Kan. Stat. Ann. §§ 50-723 - 50-724	No. Applies only to identity theft victims.	No	Jan. 1, 2007

[20] (...continued)
§ 28-51-102; Rev. Code Wash. § 19.182.160.

[21] Cal. Civ. Code § 1788.18.

State Security Freeze Statute	Applies to All Consumers?	Credit Reporting Agency Fees for Freeze Requests?	Effective Date
Kentucky, Ky. Rev. Stat. §§ 367.363 - 367.370	Yes	Yes. No fee for identity theft victims.	July 11, 2006
Louisiana, La. Rev. Stat. §§ 9:3571.1 (H) to (Y)	Yes	Yes. No fee for identity theft victims or for seniors 62+ years old.	July 1, 2005
Maine, Me. Rev. Stat. Ann. tit. 10 § 1313-C	Yes	Yes. No fee for identity theft victims.	Feb. 1, 2006
Maryland, 2007 Md. Laws Ch. 307	Yes	Yes. No fee for identity theft victims.	Jan. 1, 2008
Minnesota, Minn. Stat. § 13C.016	Yes	Yes. No fee for identity theft victims.	Aug. 1, 2006
Mississippi, 2007 Miss. Laws ch. 585	No. Applies only to identity theft victims.	Yes	July 1, 2007
Montana, 2007 Mont. Laws ch. 138	Yes	Yes. No fee for identity theft victims.	July 1, 2007
Nebraska, 2007 Leg. Bill 674	Yes.	Yes. No fee for identity theft victims.	Sept. 1, 2007 (sections applying to employers take effect Sept. 1, 2008)
Nevada, Nev. Rev. Stat. § 598C.010, *et seq*.	Yes	Yes. No fee for identity theft victims.	Oct. 1, 2005
New Hampshire, Rev. Stat. N.H. §§ 359-B:22-B:29	Yes	Yes. No fee for identity theft victims.	Jan. 1, 2007
New Jersey, N.J. Stat. Ann. §§ 56:11-44 - 56:11-50	Yes	Yes. No fee for first request.	Jan. 1, 2006
New Mexico, 2007 N.M. Laws ch. 106	Yes.	Yes. No fee for identity theft victims or seniors 65+ years old.	July 1, 2007
New York, N.Y. Gen. Bus. Law §§ 380-a - 380-u	Yes	Yes. No fee for identity theft victims.	Nov. 1, 2006

State Security Freeze Statute	Applies to All Consumers?	Credit Reporting Agency Fees for Freeze Requests?	Effective Date
North Carolina, N.C. Gen. Stat. § 75-60, *et seq.*	Yes	Yes. No fee for identity theft victims.	Dec. 1, 2005
North Dakota, N.D. Cent. Code ch. 51-33	Yes	Yes. No fee for identity theft victims.	July 1, 2007
Oklahoma, Okla. Stat. tit. 24, § 149, *et seq.*	Yes	Yes. No fee for identity theft victims or seniors 65+ years old.	Jan. 1, 2007
Pennsylvania, 2006 Pa. Laws ch. 163	Yes	Yes. No fee for identity theft victims or seniors 65+ years old.	Jan. 1, 2007
Rhode Island, R.I. Gen. Laws §§ 6-48-1 - 6-48-9	Yes	Yes. No fee for identity theft victims or seniors 65+ years old.	Jan. 1, 2007
South Dakota, S.D. Codified Laws §§ 54-15-1, *et seq.*	No. Applies to identity theft victims only.	No	July 1, 2006
Tennessee, 2007 Tenn. Pub. Act ch. 170 (to be codified at Tenn. Code Ann. tit. 46, ch. 18, part 21)	Yes	Yes. Fee not to exceed $7.50. No fee for identity theft victims.	Jan. 1, 2008
Texas, Tex. Bus. & Com. Code §§ 20.031-20.04	No. Applies to identity theft victims only.	Yes. No fee for identity theft victims.	Sept. 1, 2003
Utah, Utah Code Ann. § 13-42-102 and §§ 13-45-201 - 13-45-205	Yes	Yes. Allows for "reasonable fees." No fee for identity theft victims.	Sept. 1, 2008
Vermont, Vt. Stat. Ann. tit. 9, §§ 2480a-2480j	Yes	No	July 1, 2005
Washington, Wash. Rev. Code §§ 19.182.170 - 19.182-200	No. Applies to identity theft victims.	No	July 24, 2005
W. Va. Code § 46A-6L-102	Yes	Yes. No fee for identity theft victims.	June 8, 2007

State Security Freeze Statute	Applies to All Consumers?	Credit Reporting Agency Fees for Freeze Requests?	Effective Date
Wisconsin, Wis. Stat. § 100.54	Yes	Yes. No fee for identity theft victims.	Jan. 1, 2007
Wyoming, Wyo. Stat. §§ 40-12-502 - 40-12-506	Yes	Yes. No fee for identity theft victims.	July 1, 2007

Source: Lexis.com and state government websites.

Social Security Numbers

Several state laws are intended to protect consumers' Social Security numbers (SSNs) from identity theft.[22] Michigan's Social Security Number Privacy Act, the first state law of its kind, requires employers to adopt a policy to insure the confidentiality of employee SSNs.[23] The employer policy must include document destruction protocols and impose penalties on persons who violate the policy. The statute requires employers to publish the policy in an employee handbook or through other means. California also has enacted a statute intended to protect the integrity of employees' SSNs.[24] The statute prohibits employers from publicly displaying SSNs or printing the numbers on employee identification cards or badges. Other states have restricted the collection of SSNs for use in consumer transactions. In Rhode Island, for example, it is a misdemeanor to require a consumer to disclose his or her SSN, "incident to the sale of consumer goods or services."[25] The law includes exceptions for insurance and healthcare services and applications for consumer credit.

Proposed Federal Identity Theft Legislation

Several bills have been introduced in the 110th Congress to combat identity theft, address security breaches, and protect personal information. Summaries of the bills provided below are from the Legislative Information System [http://www.congress.gov].

---

[22] For further information, see CRS Report RL30318, *The Social Security Number: Legal Developments Affecting Its Collection, Disclosure, and Confidentiality*, by Kathleen S. Swendiman.

[23] Mich. Comp. Laws. § 445.84.

[24] Cal. Civ. Code §§ 1798.85-1798.86.

[25] R.I. Gen. Laws § 6-13-17.

H.R. 136 (Gallegly)

Identity Theft Notification Act of 2007. This bill would amend title II (Old Age, Survivors and Disability Insurance) of the Social Security Act to require the Commissioner of Social Security to notify individuals and appropriate authorities of evidence of a certain misuse of individual Social Security account numbers. The bill also requires the Commissioner to determine, in certain instances of wage reports involving multiple addresses for the same employee name, whether there is evidence that the wages were not paid to the individual to whom the Social Security account number was assigned.

H.R. 138 (Gallegly)

Employment Eligibility Verification and Anti-Identity Theft Act. This bill would direct the Commissioner of the Social Security Administration to notify a person or entity each time that the combination of name and Social Security account number it has submitted for an individual does not match Social Security Administration records. The bill also directs the Secretary of the Department Homeland Security (DHS) to notify a person or entity each time that (1) an immigration status or employment authorization document presented or referenced by an individual during the employment eligibility verification process was assigned to another person; or (2) there is no agency record that the document was assigned to any person. Additionally, the bill directs the DHS Secretary to establish a system, meeting specified requirements, for verifying an individual's identity and employment eligibility. Requires any person or entity that has received a discrepancy notice under this act to verify the individual's employment authorization and identity through such system. The bill places the burden of resolving errors in the verification mechanism on the individual whose employment eligibility and identity have not been verified and requires the individual to terminate any employment in the United States if a final nonverification is received. The bill also requires the Commissioner of Social Security to provide the last known name, address, and location of a nonverified individual to the Secretary of DHS and provides for sanctions against employers who continue to employ an individual after receiving a final nonverification. The bill also amends the Illegal Immigration Reform and Immigrant Responsibility Act of 1996 to require any person or entity that receives written notice about more than 20 individuals in one calendar year to (1) participate in a basic pilot project for employment eligibility confirmation; and (2) comply with specified terms and conditions. The bill also provides for (1) a remedy under the Federal Tort Claims Act for job dismissals occasioned by verification mechanism errors; and (2) protection from civil and criminal liability for persons or entities that take action in good faith on the basis of verification mechanism information.

H.R. 220 (Paul)

Identity Theft Protection Act of 2007. This bill would amend title II (Old Age, Survivors and Disability Insurance) of the Social Security Act and the Internal Revenue Code to prohibit using a Social Security account number except for specified Social Security and tax purposes. The bill also prohibits the Social Security Administration from divulging the Social Security account number of an individual to any federal, state, or local government agency or instrumentality, or to any other individual. Additionally, the bill amends the Privacy Act of 1974 to prohibit any federal, state, or local government agency or instrumentality from requesting an individual to disclose his Social Security account number on either a mandatory or

a voluntary basis and prohibits any two federal agencies or instrumentalities from implementing the same identifying number with respect to any individual (except as authorized by the Social Security Act). The bill also prohibits any federal agency from (1) establishing or mandating a uniform standard for identification of an individual that is required to be used by any other federal or state agency, or by a private person, for any purpose other than that of conducting the authorized activities of the standard-establishing or -mandating federal agency; or (2) conditioning receipt of any federal grant, contract, or other federal funding on the adoption, by a state or local government, or by a state agency, of such a uniform standard.

H.R. 246 (Reichert)

Methamphetamine and Identity Theft Study Act of 2007. This bill would direct the Attorney General to conduct a study evaluating whether there is a connection between the commission of crimes involving methamphetamine and the commission of identity theft crimes. The bill also requires such study to include a statistical analysis of any correlation and to evaluate (1) imposing a sentencing enhancement if a person commits both; (2) establishing a password-protected electronic clearinghouse within the Department of Justice for federal, state, and local law enforcement agencies to share information on crimes involving both; and (3) whether individuals who use methamphetamine are more likely to commit certain kinds of identity theft crimes, such as through the use of mail, than are others who commit identity theft crimes.

H.R. 336 (S. Davis)

Identity Theft Protection and Timely Reporting Act of 2007. This bill would direct the National Technical Information Service of the Department of Commerce to provide monthly updates of the Death Master List prepared by the Social Security Administration to each consumer reporting agency described in the Fair Credit Reporting Act. The bill also amends the Fair Credit Reporting Act to require each such consumer reporting agency to include a fraud alert in the consumer file of each consumer whose name appears on the Death Master List prepared by the Social Security Administration so long as the agency continues to maintain such file.

H.R. 531 (Lynch)

Retirement Security Education Act of 2007. This bill would authorize the Secretary of Health and Human Services to award grants to eligible entities to provide financial education programs to mid-life and older individuals who reside in local communities in order to (1) enhance their financial and retirement knowledge; and (2) reduce financial abuse and fraud, including telemarketing, mortgage, and pension fraud, among them. The bill also authorizes the Secretary to award a grant to one or more eligible entities to (1) create and make available instructional materials and information that promote financial education; and (2) provide training and other related assistance regarding the establishment of financial education programs. Additionally, the bill expresses the sense of Congress that organizations with demonstrated experience in providing financial education to older women should receive high priority for assistance under this act.

H.R. 605 (Hayes)

Seniors Taking on Phony Marketers Act of 2007. This bill would amend the federal criminal code to increase from 10 to 15 years the additional term of

imprisonment for telemarketing fraud aimed at individuals over the age of 55. The bill also authorizes appropriations for FY2008 for (1) 50 new postal inspectors to investigate telemarketing fraud; (2) 30 new assistant U.S. attorneys to prosecute telemarketing fraud cases; and (3) public awareness and prevention initiatives to educate senior citizens about telemarketing fraud.

H.R. 836 (L. Smith)

Cyber-Security Enhancement and Consumer Data Protection Act of 2007. This bill would amend the federal criminal code to (1) prohibit accessing or remotely controlling a protected computer to obtain identification information; (2) revise the definition of "protected computer" to include computers affecting interstate or foreign commerce or communication; (3) expand the definition of racketeering to include computer fraud; (4) redefine the crime of computer-related extortion to include threats to access without authorization (or to exceed authorized access of) a protected computer; (5) impose criminal penalties for conspiracy to commit computer fraud; (6) impose a fine and/or five year prison term for failure to notify the U.S. Secret Service or Federal Bureau of Investigation (FBI) of a major security breach (involving a significant risk of identity theft) in a computer system, with the intent to thwart an investigation of such breach; (7) increase to 30 years the maximum term of imprisonment for computer fraud and require forfeiture of property used to commit computer fraud; and (8) impose criminal penalties for damaging 10 or more protected computers during any one-year period. The bill also directs the U.S. Sentencing Commission to review and amend its guidelines and policy statements to reflect congressional intent to increase criminal penalties for computer fraud and authorizes additional appropriations in FY2007-FY2011 to the U.S. Secret Service, the Department of Justice, and the FBI to investigate and prosecute criminal activity involving computers.

H.R. 948 (Markey)

Social Security Number Protection Act of 2007. This bill would amend title II (Old Age, Survivors and Disability Insurance) of the Social Security Act (SSA) to make it unlawful for any person to sell or purchase a Social Security number in a manner that violates a regulation promulgated by the Federal Trade Commission (FTC), except in certain circumstances.

H.R. 958 (Rush)

Data Accountability and Trust Act. This bill would require the Federal Trade Commission (FTC) to promulgate regulations requiring each person engaged in interstate commerce that owns or possesses electronic data containing personal information to establish security policies and procedures. The bill also authorizes the FTC to require a standard method or methods for destroying obsolete nonelectronic data. The bill also requires information brokers to submit their security policies to the FTC in conjunction with a security breach notification or on FTC request, requires the FTC to conduct or require an audit of security practices when information brokers are required to provide notification of such a breach, and authorizes additional audits after a breach. Additionally, the bill requires information brokers to (1) establish procedures to verify the accuracy of information that identifies individuals; (2) provide to individuals whose personal information it maintains a means to review it; (3) place notice on the Internet instructing individuals how to request access to such information; and (4) correct inaccurate information.

Furthermore, the bill directs the FTC to require information brokers to establish measures which facilitate the auditing or retracing of access to, or transmissions of, electronic data containing personal information and prohibits information brokers from obtaining or disclosing personal information by false pretenses (pretexting). Additionally, the bill prescribes procedures for notification to the FTC and affected individuals of information security breaches. The bill also sets forth special notification requirements for breaches (1) by contractors who maintain or process electronic data containing personal information; (2) involving telecommunications and computer services; and (3) of health information. H.R. 958 preempts state information security laws.

H.R. 1008 (Bean)

Safeguarding America's Families by Enhancing and Reorganizing New and Efficient Technologies (SAFER NET) Act of 2007. This bill would require the Federal Trade Commission (FTC) to establish an Office of Internet Safety and Public Awareness to be headed by a Director. The bill requires the FTC, acting through the Office, to carry out a nationwide program to increase public awareness and education regarding Internet safety, that utilizes existing resources and efforts of all levels of government and other appropriate entities and that includes (1) evaluating and improving the efficiency of Internet safety efforts provided by such entities; (2) identifying and promoting best practices; (3) establishing and carrying out a national outreach and education campaign; (4) serving as the primary contact in the federal government and as a national clearinghouse for Internet safety information; (5) facilitating access to, and the exchange of, such information; (6) providing expert advice to the FTC; and (7) providing technical, financial, and other appropriate assistance to such entities.

H.R. 1307 (H. Wilson)

Veterans Identity Protection Act. This bill would establish as an independent office in the executive branch, the Office of Veterans Identity Protection Claims, headed by a Director, to receive, process, and pay claims for injuries suffered as a result of the unauthorized use, disclosure, or dissemination of identifying information stolen from the Department of Veterans Affairs (VA) or otherwise compromised as a result of a security breach. The bill also authorizes judicial review of claim determinations.

H.R. 1525 (Lofgren)

Internet Spyware (I-SPY) Prevention Act. This bill would amend the federal criminal code to prohibit intentionally accessing a protected computer without authorization, or exceeding authorized access, by causing a computer program or code to be copied onto the protected computer, and intentionally using that program or code (1) in furtherance of another federal criminal offense; (2) to obtain or transmit personal information (including a Social Security number or other government-issued identification number, a bank or credit card number, or an associated password or access code) with intent to defraud or injure a person or cause damage to a protected computer; or (3) to impair the security protection of that computer. The bill also prohibits any person from bringing a civil action under state law premised upon the defendant's violating this act. Additionally, the bill provides that this act does not prohibit any lawfully authorized investigative, protective, or intelligence activity of a law enforcement agency or a U.S. intelligence agency. The

bill also authorizes appropriations to the Attorney General for prosecutions needed to discourage the use of spyware and the practices called phishing and pharming and expresses the sense of Congress that the Department of Justice should vigorously prosecute those who use spyware to commit crimes and those that conduct phishing and pharming scams. The House Committee on the Judiciary issued H.Rept. 110-159 on the bill on May 21, 2007.

H.R. 1860 (McCarthy)

Identity Theft Relief Act of 2007. This bill would amend the Internal Revenue Code of 1986 by adding Section 224, *Expenses Related to Identity Theft*. Section 224 allows an individual to deduct all ordinary and necessary expenses paid or incurred during the taxable year, not compensated for by insurance or otherwise, in connection with a qualified identity theft.

H.R. 3046 (McNulty)

Social Security Number Privacy and Identity Theft Prevention Act of 2007. This bill would amend the Social Security Act to enhance Social Security account number privacy protections, to prevent fraudulent misuse of the Social Security account number, and to enhance protection against identity theft. The bill would prohibit the sale or display of Social Security numbers by the government to the general public. Additionally, the bill would create new criminal and civil penalties for the sale or misuse of Social Security numbers or for counterfeiting Social Security cards. It also would create new criminal and civil penalties for Social Security Administration employees who fraudulently issue Social Security numbers or cards. Penalties are enhanced in cases of terrorism, drug trafficking, crimes of violence, or prior offenses. The bill includes exceptions for law enforcement and national security; for compliance with tax laws; and for research "for the purpose of advancing public good," including medical research. The bill also would prohibit access by prison inmates to the Social Security numbers of others.

S. 238 (Feinstein)

Social Security Number Misuse Prevention Act. This bill would amend the federal criminal code to prohibit the display, sale, or purchase of Social Security numbers without the affirmatively expressed consent of the individual, except in specified circumstances. It also directs the Attorney General to study and report to Congress on all the uses of Social Security numbers permitted, required, authorized, or excepted under any federal law, including the impact of such uses on privacy and data security. Additionally, the bill establishes a public records exception to the prohibition and directs the Comptroller General to study and report to Congress on Social Security numbers in public records. The bill also grants the Attorney General rulemaking authority to enforce this act's prohibition and to implement and clarify the permitted uses occurring as a result of an interaction between businesses, governments, or business and government. The bill also amends title II (Old Age, Survivors, and Disability Insurance) of the Social Security Act (SSA) to prohibit (1) the use of Social Security numbers on checks issued for payment by governmental agencies; and (2) inmate access to Social Security account numbers. The bill prohibits a commercial entity from requiring an individual to provide a Social Security number when purchasing a commercial good or service or denying an individual the good or service for refusing to provide that number, with exceptions.

The bill both establishes civil and criminal penalties and extends civil monetary penalties for misuse of a Social Security number and provides for (1) criminal penalties under SSA title II for the misuse of a Social Security number; (2) civil actions and civil penalties against persons who violate this act; and (3) federal injunctive authority with respect to any violation by a public entity.

S. 239 (Feinstein)

Notification of Risk to Personal Data Act of 2007. This bill would require any federal agency or business entity engaged in interstate commerce that uses, accesses, transmits, stores, disposes of, or collects sensitive, personally identifiable information, following the discovery of a security breach, to notify (as specified): (1) any U.S. resident whose information may have been accessed or acquired; and (2) the owner or licensee of any such information the agency or business does not own or license. Additionally, the bill exempts (1) agencies from notification requirements for national security and law enforcement purposes and for security breaches that do not have a significant risk of resulting in harm, provided specified certification or notice is given to the U.S. Secret Service; and (2) business entities from notification requirements if the entity utilizes a security program that blocks unauthorized financial transactions and provides notice of a breach to affected individuals. The bill also requires notifications regarding security breaches under specified circumstances to the Secret Service, the Federal Bureau of Investigation, the United States Postal Inspection Service, and state attorneys general. Furthermore, the bill sets forth enforcement provisions and authorizes appropriations for costs incurred by the Secret Service to investigate and conduct risk assessments of security breaches. The Senate Committee on the Judiciary reported the bill without a written report on May 31, 2007.

S. 495 (Leahy)

Personal Data Privacy and Security Act of 2007. This bill would amend the federal criminal code to (1) make fraud in connection with the unauthorized access of sensitive personally identifiable information (in electronic or digital form) a predicate for racketeering charges; and (2) prohibit concealment of security breaches involving such information. The bill also directs the U.S. Sentencing Commission to review and amend its guidelines relating to fraudulent access to, or misuse of, digitized or electronic personally identifiable information (including identify theft). Additionally, the bill requires a data broker to (1) disclose to an individual, upon request, personal electronic records pertaining to such individual maintained for disclosure to third parties; and (2) maintain procedures for correcting the accuracy of such records. The bill also establishes standards for developing and implementing safeguards to protect the security of sensitive personally identifiable information. Additionally, the bill imposes upon business entities civil penalties for violations of such standards and requires such business entities to notify (1) any individual whose information has been accessed or acquired; and (2) the U.S. Secret Service if the number of individuals involved exceeds 10,000. Furthermore, the bill authorizes the Attorney General and state attorneys general to bring civil actions against business entities for violations of this act. The bill requires the Administrator of the General Services Administration in considering contract awards totaling more than $500,000, to evaluate (1) the data privacy and security program of a data broker; (2) program compliance; (3) the extent to which databases and systems have been compromised by security breaches; and (4) data broker responses to such breaches. The bill also

requires federal agencies to conduct a privacy impact assessment before purchasing personally identifiable information from a data broker. The Senate Committee on the Judiciary reported out S.Rept. 110-70 on May 23, 3007.

S. 699 (Allard)

Social Security Number Fraud and Identity Theft Prevention Act. This bill would amend the Immigration and Nationality Act to authorize the Secretary of the Department of Homeland Security (DHS), the Secretary of Labor, and the Attorney General to require an individual to provide the individual's Social Security account number for inclusion in any (1) record of the individual maintained by either such Secretary or the Attorney General; or (2) any application, document, or form provided under or required by the immigration laws. (Currently, the Attorney General is authorized to require any alien to provide a Social Security account number for inclusion in any record maintained by the Attorney General or the Bureau of Citizenship and Immigration Services.) The bill also requires the Commissioner of Social Security to provide the DHS Secretary with information regarding the name, date of birth, and address of each individual who used the same Social Security account number, and the name and address of the person reporting the earnings for each such individual. Additionally, the bill requires the Commissioner to provide such information to the DHS Secretary, in an electronic form, if more than one person reports earnings for an individual during a single tax year. The bill directs the Commissioner, at the DHS Secretary's request and expense, to perform and report on a search or manipulation of Social Security Commission records if the Secretary certifies that the purpose is to obtain information likely to assist in identifying individuals (and their employers) who are (1) using false names or Social Security account numbers; (2) sharing a single valid name and Social Security account number among multiple individuals; (3) using the Social Security account number of a person who is deceased, too young to work, or not authorized to work; or (4) otherwise engaged in a violation of the immigration laws. Furthermore, the bill declares inadmissible to receive visas and to be admitted to the United States any alien who falsely represents himself or herself to be a U.S. national for any purpose or benefit under immigration and nationality or any other federal or state law.

S. 806 (Pryor)

Consumer ID Protection and Security Act. This bill would authorize a consumer to place a security freeze on his or her credit report by making a request to a consumer credit reporting agency in writing, by telephone, or through a secure electronic connection if such a connection is made available by the agency, subject to specified requirements.

S. 1178 (Inouye)

Identity Theft Prevention Act. This bill would require any commercial entity or charitable, educational, or nonprofit organization that acquires, maintains, or uses sensitive personal information (covered entity) to develop, implement, maintain, and enforce a written program, containing administrative, technical, and physical safeguards, for the security of sensitive personal information it collects, maintains, sells, transfers, or disposes of. The bill defines "sensitive personal information" as an individual's name, address, or telephone number combined with at least one of the following relating to that individual: (1) the social security number or numbers derived from that number; (2) financial account or credit or debit card numbers

combined with codes or passwords that permit account access, subject to exception; or (3) a state driver's license or resident identification number. The proposed act requires a covered entity (1) to report a security breach to the Federal Trade Commission (FTC); (2) if the entity determines that the breach creates a reasonable risk of identity theft, to notify each affected individual; and (3) if the breach involves at least 1,000 individuals, to notify all consumer reporting agencies specified in the Fair Credit Reporting Act. The bill also authorizes a consumer to place a security freeze on his or her credit report by making a request to a consumer credit reporting agency, and prohibits a reporting agency, when a freeze is in effect, from releasing the consumer's report for credit review purposes without the consumer's prior express authorization. Additionally, this legislation requires (1) the establishment of the Information Security and Consumer Privacy Advisory Committee; (2) a related crime study, including the correlation between methamphetamine use and identity theft crimes. Also, this bill treats any violation of this act as an unfair or deceptive act or practice under the Federal Trade Commission Act, requires enforcement under other specified laws, allows enforcement by state attorneys general, and preempts state laws requiring notification of affected individuals of security breaches.

S. 1202 (Sessions)

Personal Data Protection Act of 2007. This bill would require agencies and individuals who possess computerized data containing sensitive personal information to disclose security breaches that pose a significant risk of identity theft.