S 1178

Identity Theft Prevention Act

Congress: 110 (2007–2009, Ended)
Chamber: Senate
Policy Area: Commerce
Introduced: Apr 20, 2007
Current Status: Placed on Senate Legislative Calendar under General Orders. Calendar No. 520.
Latest Action: Placed on Senate Legislative Calendar under General Orders. Calendar No. 520. (Dec 5, 2007)
Official Text: https://www.congress.gov/bill/110th-congress/senate-bill/1178

Sponsor

Name: Sen. Inouye, Daniel K. [D-HI]
Party: Democratic • **State:** HI • **Chamber:** Senate

Cosponsors (4 total)

Cosponsor	Party / State	Role	Date Joined
Sen. Pryor, Mark L. [D-AR]	D · AR		Apr 20, 2007
Sen. Smith, Gordon H. [R-OR]	R · OR		Apr 20, 2007
Sen. Stevens, Ted [R-AK]	R · AK		Apr 20, 2007
Sen. Nelson, Bill [D-FL]	D · FL		Apr 24, 2007

Committee Activity

Committee	Chamber	Activity	Date
Commerce, Science, and Transportation Committee	Senate	Reported By	Dec 5, 2007

Subjects & Policy Tags

Policy Area:

Commerce

Related Bills

Bill	Relationship	Last Action
110 S 806	Related bill	**Mar 7, 2007:** Read twice and referred to the Committee on Banking, Housing, and Urban Affairs.

Summary (as of Dec 5, 2007)

Identity Theft Prevention Act - (Sec. 2) Requires 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. 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.

(Sec. 3) 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 1,000 or more individuals, to notify all consumer reporting agencies specified in the Fair Credit Reporting Act.

(Sec. 4) Authorizes a consumer to place a security freeze on his or her credit report by making a request to a consumer credit reporting agency. 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. Provides for freeze removal and suspension, limits related fees, and sets forth other security freeze requirements. Exempts from certain provisions of this Act: (1) a consumer credit reporting agency that acts only as a reseller of credit information and does not maintain a permanent database of credit information; (2) check services or fraud prevention services companies; and (3) deposit account information service companies.

(Sec. 5) Requires: (1) the establishment of the Information Security and Consumer Privacy Advisory Committee; and (2) a related crime study and report, including regarding the correlation between methamphetamine use and identity theft crimes.

(Sec. 8) 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. Preempts state laws requiring notification of affected individuals of security breaches. Preempts state laws relating to the use of social security numbers.

(Sec. 11) Prohibits, subject to exception, a covered entity from soliciting a social security number from an individual unless there is a specific use of that number for which no other identifier can reasonably be used.

Prohibits the display of social security numbers on identification cards commonly provided to employees, faculty, staff, or students and on state driver's licenses.

Amends title II (Old Age, Survivors and Disability Insurance) (OASDI) of the Social Security Act to prohibit federal, state, and political subdivision governmental entities and their agents from using prisoners in a way that would allow the prisoners access to other individuals' social security numbers.

Makes it unlawful to sell, purchase, provide, or display a social security number to the general public or to obtain or use any individual's social security number for the purpose of locating or identifying the individual with the intent to physically injure or harm the individual or for the purpose of using the individual's identity for any illegal purpose, subject to exceptions, including sales or displays of such numbers for the purposes of national security, public health or safety, and

locating abducted children.

(Sec. 12) Requires each U.S. agency to: (1) develop, implement, maintain, and enforce a written program for the security of sensitive personal information the agency collects, maintains, sells, transfers, or disposes of; (2) use due diligence to investigate any suspected breach of security affecting sensitive personal information; and (3) notify each affected individual after a breach.

(Sec. 14) Authorizes appropriations.

Actions Timeline

- **Dec 5, 2007:** Committee on Commerce, Science, and Transportation. Reported by Senator Inouye with amendments. With written report No. 110-235.
- **Dec 5, 2007:** Placed on Senate Legislative Calendar under General Orders. Calendar No. 520.
- **Apr 25, 2007:** Committee on Commerce, Science, and Transportation. Ordered to be reported with amendments favorably.
- **Apr 20, 2007:** Introduced in Senate
- **Apr 20, 2007:** Sponsor introductory remarks on measure. (CR S4812-4813)
- **Apr 20, 2007:** Read twice and referred to the Committee on Commerce, Science, and Transportation.