# HR 2221

Data Accountability and Trust Act

**Congress:** 111 (2009–2011, Ended)
**Chamber:** House
**Policy Area:** Commerce
**Introduced:** Apr 30, 2009
**Current Status:** Received in the Senate and Read twice and referred to the Committee on Commerce, Science, and Transp
**Latest Action:** Received in the Senate and Read twice and referred to the Committee on Commerce, Science, and Transportation. (Dec 9, 2009)
**Official Text:** https://www.congress.gov/bill/111th-congress/house-bill/2221

## Sponsor

**Name:** Rep. Rush, Bobby L. [D-IL-1]
**Party:** Democratic • **State:** IL • **Chamber:** House

## Cosponsors (4 total)

| Cosponsor | Party / State | Role | Date Joined |
|---|---|---|---|
| Rep. Barton, Joe [R-TX-6] | R · TX | | Apr 30, 2009 |
| Rep. Radanovich, George [R-CA-19] | R · CA | | Apr 30, 2009 |
| Rep. Schakowsky, Janice D. [D-IL-9] | D · IL | | Apr 30, 2009 |
| Rep. Stearns, Cliff [R-FL-6] | R · FL | | Apr 30, 2009 |

## Committee Activity

| Committee | Chamber | Activity | Date |
|---|---|---|---|
| Commerce, Science, and Transportation Committee | Senate | Referred To | Dec 9, 2009 |
| Energy and Commerce Committee | House | Reported by | Jun 3, 2009 |

## Subjects & Policy Tags

**Policy Area:**

Commerce

## Related Bills

| Bill | Relationship | Last Action |
|---|---|---|
| 111 S 3742 | Related bill | **Sep 22, 2010:** Committee on Commerce, Science, and Transportation Subcommittee on Consumer Protection, Product Safety, and Insurance . Hearings held. With printed Hearing: S.Hrg. 111-1040. |

## Summary (as of Dec 8, 2009)

Data Accountability and Trust Act - (Sec. 2) Requires the Federal Trade Commission (FTC) to promulgate regulations requiring each person engaged in interstate commerce owning or possessing electronic data containing personal information, or contracting with a third party to maintain such data, to establish security policies and procedures.

Requires such policies and procedures to provide for: (1) a security policy with respect to the use, sale, dissemination, and maintenance of data; (2) an officer responsible for information security oversight; (3) vulnerability testing of security programs; and (4) a process for disposing of obsolete electronic and non-electronic data containing personal information.

Deems an information broker to be in compliance with the appropriate provisions of this Act if such broker is in compliance with: (1) any other federal information security statutes which provide similar or greater protections than those required under this Act; or (2) relevant provisions of the Fair Credit Reporting Act (FCRA).

Requires information brokers to submit their security policies to the FTC in conjunction with a security breach notification or on FTC request. Authorizes the FTC to conduct audits of the information security practices of such information broker, or require independent audits of their practices.

Requires information brokers to: (1) establish procedures to verify the accuracy of collected information that specifically identifies individuals; (2) provide annually, and without cost, to individuals whose personal information it maintains a means to review it; (3) place a notice on the Internet instructing individuals how to request access to such information; (4) correct inaccurate information upon request; and (5) in the case of information brokers that do use data for marketing purposes, allow individuals to decide if their information can be used.

Sets forth limitations to such access rights and website notice requirements.

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.

Prohibits information brokers from obtaining or disclosing, or soliciting to obtain, personal information by false pretenses (pretexting).

Exempts from the provisions of this section a service provider serving only as the conduit for the transmission, routing, or transient storage of information.

(Sec. 3) Requires any person engaged in interstate commerce owning or possessing data in electronic form to notify, within 60 days following the discovery of a security breach: (1) the FTC; and (2) each individual whose personal information was acquired or accessed.

Requires a third party agent maintaining or processing personal information in electronic form to notify the person owning or possessing the data in the event of a security breach.

Requires a service provider transmitting, routing, or providing transient routing of personal information owned or possessed by another person to notify the person who initiated the connection or transmission in the event of a security breach.

Requires a person required to provide notification to more than 5,000 individuals to notify the major credit reporting agencies of the timing and distribution of the notices.

Sets forth notification provisions, including: (1) notification timeliness and content; (2) notification delay for law enforcement or national security purposes when notification would threaten law enforcement or national security; and (3) substitute notification.

Requires a person providing notice to individuals to provide consumer credit reports or a credit monitoring service that enables consumers to detect misuse of their personal information.

Exempts a person from such notification requirements if following a security breach a person determines that there is no reasonable risk of identity theft, fraud, or other unlawful conduct.

Establishes a presumption that there is no reasonable risk of identity theft, fraud, or other unlawful conduct if the personal information in electronic form subject to a security breach is unusable, unreadable, or indecipherable to an unauthorized third party. Directs the FTC to issue rules identifying security methodologies or technologies which render data unusable, unreadable, or indecipherable for the purpose of establishing such presumption.

Directs the FTC to: (1) place a security breach notice on its website if in the public interest; and (2) study the practicality and cost effectiveness of providing notice in languages in addition to English.

(Sec. 4) Limits the application of sections 2 and 3 of this Act to persons, partnerships, or corporations over which the FTC has authority pursuant to its authority to prevent unfair methods of competition and unfair or deceptive acts or practices in or affecting commerce.

States that a violation of section 2 or 3 shall be treated as an unfair and deceptive act or practice.

Prohibits the FTC, when promulgating rules under this Act, from requiring the deployment or use of any specific products or technologies.

Provides for civil action enforcement by the attorney general of a state, or an official or agency of a state, for violations of section 2 and 3. Sets forth: (1) methods for calculating civil penalties; and (2) limitations and obligations on state actions.

Establishes as an affirmative defense to certain enforcement or civil actions under this section that all of the personal information compromised in a particular security breach is lawfully acquired public record information.

(Sec. 5) Defines "information broker" as: (1) a commercial entity (or its contractor or subcontractor) whose business is to collect, assemble, or maintain personal information concerning individuals who are not current or former customers of such entity in order to sell or provide access to such information to any nonaffiliated third party. States that such definition does not include a commercial entity to the extent that such entity processes information collected by or on behalf of and received from or on behalf of a nonaffiliated third party concerning individuals who are current or former customers or employees of such third party to enable such third party to provide benefits for its employees or transact business with its customers.

Defines "personal information" as an individual's first name or initial and last name, address, or phone number, in combination with any one or more of the following data elements: (1) social security number; (2) driver's license number, passport number, military identification number, or other government-issued identity document; and (3) financial account number or credit or debit card number and any related security access code or password.

Defines "service provider" as a person providing electronic data transmission, routing, intermediate and transient storage, or connections to its system, where the person providing such services does not select or modify the content of the

electronic data, is not the sender or the intended recipient of the data, and such person transmits, routes, stores, or provides connections for personal information in a manner that personal information is undifferentiated from other types of data.

(Sec. 6) Preempts any provision of a state law to the extent that the state law requires: (1) information security practices and treatment of data containing personal information similar to any of those required under section 2 of this Act; and (2) notification to individuals of a security breach resulting in unauthorized access to or acquisition of electronic data containing personal information.

Prohibits any person other than a person specified in section 4 of this Act from bringing a civil action under state law if such action is premised upon the defendant violating any provisions of this Act. (States that this provision shall not be construed to limit the enforcement of any state consumer protection law by an attorney general of a state.)

States that this Act shall not be construed to: (1) limit FTC authority; or (2) preempt state trespass, contract, tort, or fraud law.

(Sec. 7) Makes this Act effective one year after its enactment.

(Sec. 8) Authorizes FY2010-FY2015 appropriations to carry out this Act.

## Actions Timeline

- **Dec 9, 2009:** Received in the Senate and Read twice and referred to the Committee on Commerce, Science, and Transportation.
- **Dec 8, 2009:** Reported (Amended) by the Committee on Energy and Commerce. H. Rept. 111-362.
- **Dec 8, 2009:** Placed on the Union Calendar, Calendar No. 214.
- **Dec 8, 2009:** Mr. Rush moved to suspend the rules and pass the bill, as amended.
- **Dec 8, 2009:** Considered under suspension of the rules. (consideration: CR H13586-13591)
- **Dec 8, 2009:** DEBATE - The House proceeded with forty minutes of debate on H.R. 2221.
- **Dec 8, 2009:** Passed/agreed to in House: On motion to suspend the rules and pass the bill, as amended Agreed to by voice vote.(text: CR H13586-13590)
- **Dec 8, 2009:** On motion to suspend the rules and pass the bill, as amended Agreed to by voice vote. (text: CR H13586-13590)
- **Dec 8, 2009:** Motion to reconsider laid on the table Agreed to without objection.
- **Dec 8, 2009:** The title of the measure was amended. Agreed to without objection.
- **Sep 30, 2009:** Committee Consideration and Mark-up Session Held.
- **Sep 30, 2009:** Ordered to be Reported (Amended) by Voice Vote.
- **Jun 3, 2009:** Subcommittee Consideration and Mark-up Session Held.
- **Jun 3, 2009:** Forwarded by Subcommittee to Full Committee (Amended) by Voice Vote .
- **May 5, 2009:** Subcommittee Hearings Held.
- **May 1, 2009:** Referred to the Subcommittee on Commerce, Trade and Consumer Protection.
- **Apr 30, 2009:** Introduced in House
- **Apr 30, 2009:** Referred to the House Committee on Energy and Commerce.