Consumers Union
Nonprofit Publisher of Consumer Reports

Two Key House Bills on Data Privacy and Identity Theft

Two bills with radically different consequences for consumers have passed out of committee in the House. These bills are the weak H.R. 3997, which has been reported out of the House Financial Services Committee, and the stronger H.R. 4127, which was unanimously reported out by the House Energy and Commerce.

Consumers Union joined with many other public interest groups in strongly opposing H.R. 3997, and we believe that consumers would be worse off if such a bill becomes law than if Congress takes no action at all. A much better outcome would for the House to move H.R. 4127, a bill supported by Consumers Union as a balanced and moderate approach to data security issues.

This summary reviews the major data privacy and identity theft issues under debate in the 109th Congress and summarizes how H.R. 3997 and H.R. 4127 address them. It also provides a list of the key features of these and other bills under active consideration in the House and Senate.

Key issues in the federal debate and differences between the two House vehicles (H.R. 3997 and H.R. 4127)

- **Notice of breach to individuals.** Individuals need to be notified when the security of their unsecured, sensitive personal information (*e.g.,* Social Security number, date of birth, financial account number, etc.) has been breached, so that they can take reasonable steps to prevent or detect identity theft. In addition, when companies know they will have to notify individuals when data has been compromised, those companies have more of an incentive to take effective preventative steps to protect the data from being breached in the first place.

  H.R. 3997 requires notice only if the information whose security has been breached is reasonably likely to be misused in a manner causing harm or inconvenience to any consumer to whom the information relates. This is weaker than many state laws, which require notification each time that sensitive data is breached. Under H.R. 3997, if a company does not know whether there is a risk, then it does not have to notify individuals. We call this a "don't know, don't tell" trigger. If the recent breach involving veterans' data had occurred at a private company, the standard under H.R. 3997 would not have required notice to the veterans, because the thief's purposes were unknown.

  H.R. 4127 is also weaker than the strongest state laws, but it represents a better, and more consumer-friendly, compromise. It contains an exception rather than a trigger. That is, under H.R. 4127, companies are required to notify individuals unless they find that there is no reasonable risk of harm. When a company doesn't know whether there is harm, consumers are still notified.

- **Security freeze.** This is the most effective tool to prevent identity theft. In its strongest form, it allows each consumer the choice to "freeze" or lock his or her credit file against anyone trying to open up a new account or to get new credit in the name of the consumer. When a security freeze is in place, an identity thief can't open up a new account in the victim's name because the potential creditor or seller of services can't check the consumer's credit. A consumer may temporarily or permanently lift the freeze when he or she is applying for credit.

West Coast Office
1535 Mission Street
San Francisco, CA 94103
415.431.6747 tel
415.431.0906 fax
www.consumersunion.org

Twenty-five states have enacted security freeze laws, and twenty of those make the freeze available to all consumers. Consumers living in eleven of these twenty states have the right to put a security freeze on their files now. The nine other states have security freeze laws covering all consumers that will go into effect at a later date. Two states that initially limited the security freeze to victims only have changed their laws to expand the freeze to all consumers. H.R. 4127 leaves the issue of security freezes to the states. H.R. 3997 eliminates all state security freeze laws and replaces them with a very weak federal freeze that no one can access until after he or she has already been victimized by ID theft. This makes little sense, since the security freeze is the most effective tool to prevent becoming a victim of new account ID theft. If H.R. 3997 were current law, the more than 26 million veterans who had their unencrypted Social Security numbers and other information stolen in the VA breach would have to wait until they become victims of identity theft – too little, too late.

- **Access and correction of data broker files.** Data brokers like ChoicePoint collect and sell a wide range of information on individuals – including financial and biometric data, as well as arrest records, health, and employment records. They are unregulated, except to the extent that they are considered financial institutions under the Gramm-Leach-Bliley Act (GLBA) or are covered for specified purposes by the Fair Credit Reporting Act (FCRA). Because these institutions sell the most personal data to a wide range of clients, both public and private, it is critical that individuals be able to review this information and correct any inaccuracies. H.R. 3997 provides no right to see or dispute the contents of a data broker file. H.R. 4127 provides for both.

- **Information security safeguards.** GLBA requires that certain types of companies adopt appropriate physical, technical, and administrative safeguards on certain data. Many of the bills under consideration in the House and Senate would require that companies which hold specific types of data about individuals must have a security policy. Both H.R. 4127 and H.R. 3997 have this type of "safeguards" provision, but they would have dramatically different effects on state law. H.R. 4127 displaces only state laws requiring notice or that expressly require information security practices and treatment of data in electronic form similar to any of those required by the federal bill. H.R. 3997 displaces all state laws with "respect to the responsibilities, or the functional equivalents of such responsibilities" to "investigate and provide notices" of security breaches, "protect the security or confidentiality of information on consumers" and "safeguard such information from potential misuse."

- **Preemption.** Preemption is an important issue in the debate over identity theft, since states have led the way in providing for breach notice, security freeze laws, and other innovations. Preemption of state notice of breach laws will be less important if Congress enacts strong standards and dual enforcement for notice of security breaches. However, identity thieves are fast-acting and fast-changing, and a federal ID theft law that extends broad preemption beyond notice could prevent states from keeping up with these criminals. Congress could do much more harm than good if it enacts weak federal standards while stopping existing and new state laws.

  H.R. 4127 preempts only state laws that require notification to individuals of a security breach and state laws that require information security practices similar to those in the bill. It leaves other issues for progress by the states. H.R. 3997 broadly preempts state laws that protect the security or confidentiality of information from potential misuse, require investigation or notice of any unauthorized access to information concerning consumers, require mitigation of any loss or harm from such access or misuse, or allow consumers to place security freezes on their credit files.

- **Enforcement.** A strong enforcement mechanism provides companies with an incentive to follow the law. At the very least, any Congressional bill should allow for enforcement by state Attorneys General, to ensure that

even if federal agencies don't have the will or the resources to go after bad actors, the law can be enforced. H.R. 4127 provides for this dual enforcement by state and federal government entities; H.R. 3997 does not.

Summary of ID theft bills under active consideration in House and Senate

H.R. 4127, the Data Accountability and Trust Act (DATA) – CU Supports

- Passed House Energy & Commerce Committee.
- Lead sponsors: Representatives Stearns, Pryce of Ohio, Upton, Radanovich, Bass, Bono, Ferguson, and Blackburn.
- Notice: Individuals are notified of breaches of the security of certain personal information except where there is "no reasonable basis risk of identity theft, fraud, or other unlawful conduct."
- Security of sensitive information: Requires the FTC to establish rules for the security of personal information.
- Gives consumers free annual review of their data broker files and the right to dispute the contents of those files.
- Enforcement: Allows for enforcement by the FTC and by state AGs.
- Preemption: Displaces state laws, regulations, or rules that expressly require information security practices similar to those in the bill and state laws that require notification to individuals of a security breach. Other state laws remain undisturbed.
- Sunset: Expires ten years after the date of enactment.

H.R. 3997, Financial Data Protection Act – CU Opposes

- Passed the House Financial Services Committee.
- Lead sponsors: Representatives LaTourette, Hooley, Castle, Pryce of Ohio, and Moore of Kansas
- Scope: Applies to entities regulated by the Fair Credit Reporting Act (FCRA).
- Notice: Requires notice only if the information whose security has been breached is "reasonably likely to be misused in a manner causing harm or inconvenience to any consumer to whom the information relates." The harm must lead to a financial loss, civil or criminal penalties, or significant time and effort to correct information. The company deciding whether to give notice under this standard may consider whether security programs are likely to detect future fraudulent transactions.
- Security of sensitive information: Obligation to establish and maintain "reasonable policies" to protect the security and confidentiality of sensitive information against loss, unauthorized use, or misuse, that is reasonably likely to result in harm or inconvenience. Compliance with the Gramm-Leach-Bliley Act, where applicable, complies with this requirement.
- Security freeze: Provides security freeze for victims of ID theft only, and with respect to the credit report only. Eliminates broader state security freeze laws.
- Enforcement: No state AG enforcement; enforcement only by the functional federal regulator.
- Preemption: Preempts state laws to protect the security or confidentiality of information from potential misuse; state laws to investigate or provide notice of any unauthorized access to information concerning consumers; state laws to mitigate any loss or harm from such access or misuse, and state security freeze laws.

H.R. 5318, Cyber-Security Enhancement and Consumer Data Protection Act of 2006 – CU Supports

Passed the House Judiciary Committee
Lead Sponsors: Sensenbrenner, Coble, Smith of Texas, Feeney, Schiff and Pryce**.**
H.R. 5318 is more limited in scope than many of the other data security bills that have been passed out of committee thus far, dealing with criminal penalties and requiring notification to law enforcement officials in the event of a "major security breach," such as a breach involving information about more than 10,000 people.

S. 1789, Personal Data Privacy and Security Act – CU Supports

- Status: Passed by the Senate Judiciary Committee; awaiting action by the full Senate.
- Lead sponsors: Senators Specter, Leahy, Feinstein, and Feingold.

- Notice of breach: Individuals are notified of security breaches by businesses and federal government entities unless the breached entity submits a risk assessment in writing to the U.S. Secret Service that finds that there is no significant risk of harm. Notice also is not required when the security of financial account information such as debit or credit card numbers is compromised if the business uses a security program designed to block unauthorized transactions before they are charged to the account. Makes knowingly covering up a breach a crime.
- Security of sensitive information: Establishes standards for developing and implementing administrative, technical, and physical safeguards to protect the security of sensitive personal information.
- Data brokers: Gives individuals the right to review their data broker file for a reasonable fee, as well as the right to dispute and correct inaccuracies.
- Enforcement: Provides for enforcement by state Attorneys General (AGs).
- Preemption: Displaces state laws related to notification of a security breach, except for additional victim protection assistance provided for by state law. Eliminates all state laws relating to individual access to and correction of personal electronic records held by data brokers. Generally does not preempt state laws requiring data security unless they are inconsistent with federal law.

S. 3568, Data Security Act of 2006

- Introduced June 27, 2006, referred to the Senate Banking Committee.
- Lead sponsors: Senators Bennett and Carper.
- Notice: Requires notice only if the breached entity determines that the breach is "reasonably likely to result in substantial harm or inconvenience to the consumer." Defines substantial harm or inconvenience to require material financial loss or civil or criminal penalties due to unauthorized use of the information or the need to expend significant time and effort in order to avoid these outcomes. The company deciding whether to give notice under this standard may consider whether security programs are likely to detect future fraudulent transactions. The definition of breach excludes information in an "encrypted, redacted, altered, edited, or coded form."
- Security of sensitive information: Obligation to establish and maintain "reasonable policies" to protect the security and confidentiality of sensitive information but only from unauthorized use that is reasonably likely to result in substantial harm or inconvenience to the consumer. Compliance with the Gramm-Leach-Bliley Act, where applicable, satisfies this requirement.
- Security freeze: Silent on the security freeze. The bill appears to leave this issue to the states.
- Enforcement: No state AG enforcement; enforcement only by the functional federal regulator.
- Preemption: Preempts state laws to "protect the security or confidentiality of information relating to consumers; "state laws to "safeguard information relating to consumers from potential misuse;" and state laws to investigate or provide notice of any unauthorized access to information relating to consumers; and state laws to mitigate any loss or harm from such access or misuse.

S. 1408, Identity Theft Protection Act

- Status: Passed Senate Commerce Committee; awaiting action by the full Senate.
- Lead Sponsors: Senators Stevens, Smith, McCain, Inouye, Bill Nelson, and Pryor
- Notice of breach: Notice to individuals required only when there is a reasonable risk of identity theft.
- Security of sensitive information: Requires companies to develop, implement, maintain, and enforce a written program for the security of sensitive information.
- Security freeze: Allows all individuals to place a security freeze on their credit files for a reasonable fee set by the Federal Trade Commission (FTC).

- Social Security Number (SSN) restrictions: Prohibits the solicitation of the SSN if another identifier can reasonably be used. Prohibits display of SSN on employee or student identification card or tag. Bans sale of SSNs unless there is consent or certain other exceptions.
- Enforcement: Provides for enforcement by state AGs.
- Preemption: Displaces state laws on information security programs, notice of security breaches; state laws on solicitation or display of SSNs; and state-created liability for failure to notify of a security breach or to implement or maintain an adequate security program.

S. 1326, the "Notification of Risk to Personal Data Act" – CU Opposes
- Status: Passed Senate Judiciary Committee; awaiting action by full Senate.
- Lead Sponsor: Senator Sessions
- Notice of breach: Requires notice to individuals only "when there is a reasonable basis to conclude that a significant risk of identity theft to an individual exists." Includes a "safe harbor" provision shielding companies with existing notification policies which are consistent with the timing requirements of the Act from having to comply with other requirements of the Act including the contents of the notice and the manner of giving the notice.
- Security of sensitive information: Provides for the implementation of reasonable security standards to protect sensitive personal information from unauthorized access, destruction, use, modification, or disclosure.
- Enforcement: Allows for state AG enforcement.
- Preemption: Displaces state and local laws that relate "in any way" to electronic information security standards or individual notification of breach.

Contacts:
Susanna Montezemolo, 202.462.6262, montsu@consumer.org
Gail Hillebrand, 415.431.6747, hillga@consumer.org

7/28/06