

# **Data Security**

**By IREM Legislative Staff**

**Created November, 2006**



**Institute of Real Estate Management**

**430 N. Michigan Avenue**

**Chicago, IL 60611**

**(800) 837-0706**

*Background*

As technology has evolved and become vital for businesses, a growing number of public and private entities that keep and maintain personal information, such as financial account information, have become victims of security breaches. These breaches have exposed fundamental security flaws in the way that companies handle consumers' personal information. Individual privacy has been compromised and these breaches have put consumers at an elevated risk of becoming victims of identity theft.

The number of Congressional proposals to counteract identity theft multiplied in the spring of 2005 after ChoicePoint Inc, a commercial data broker, announced that February it may have improperly sold the personal information of almost 163,000 individuals. ChoicePoint was consequently investigated by the Federal Trade Commission. In January, 2006, the company agreed to pay \$15 million to settle charges it violated consumer privacy rights, but did not admit any wrongdoing.

Then, the substantial security breach at the U.S. Department of Veterans Affairs (VA) on May 3, 2006—widely publicized by the media—triggered more legislators on Capitol Hill to introduce data security legislation. The laptop and external disk drive, containing information on 26.5 million veterans and 1.2 million active duty personnel, of a VA employee were stolen from the employee's residence. The Secretary of the VA was not informed of the breach until May 16 and the public was not informed until May 23. The VA breach prompted legislators to narrow their focus to *when* the public should be notified if sensitive data is lost or stolen.

### ***Impact on IREM members***

In July, 2006, IREM surveyed its members holding the Certified Property Manager® (CPM) designation. The members were asked what they are currently doing and what they are willing to do to protect clients' information. Further, they were asked how they would be affected by current and future data security legislative proposals. Surprisingly, one third of CPMs had been a victim of a virus, identity theft, or hackers in the last year.

When asked if they had a written policy on data security, 37% of respondents said yes. It is in real estate managers' best interest to have a written policy. The Better Business Bureau reported 89% of customers felt more confident in giving their personal information to a business that had a detailed but readable privacy policy.

Members are relatively well informed of state laws mandating businesses provide notification to affected customers if a data breach occurs: 39% of CPMs are aware of such laws.

IREM legislative staff is taking the survey results into account when they review legislative proposals.

### ***IREM Position***

IREM has identified two main concerns with data security and consumer notification legislation. First, those bills that contain specific provisions and mechanisms that trigger notifying the consumer of a security breach, and IREM is concerned with assuring the reasonableness of the trigger mechanism and notification process. Second, the costs of compliance with state and/or federal laws would be of major concern to property managers, thus pointing to the

reasonableness thresholds above referenced. IREM encourages Congress to approve legislation which is not onerous on property owners and managers or their clients. Small businesses should not be liable for the negligent acts of third parties unless contributory negligence exists.

IREM strongly encourages its members to use best practices protect the confidential personal information of their clients.

***Legislative proposals in Congress***

Several House and Senate committees engaged in creating data security legislation during the 109th Congress. The Senate Judiciary Committee, Senate Commerce Committee, House Energy and Commerce Committee, and House Financial Services Committee each held mark-ups and passed legislation. The House and Senate are working to find compromise between varying proposals.

Existing legislative proposals primarily address jurisdictional authority, procedures to be followed by businesses when clients' sensitive personal information is stolen, or when businesses should notify their clients. Currently, over thirty states have varying laws in place. Sponsors of most of the bills introduced thus far seek to create a consistent standard preempting state laws.

IREM legislative staff is monitoring federal legislation due to its concern commercial real estate professionals could be included in the scope of the legislation and real estate managers would have to comply by notifying clients when data is breached.

***See the attached two-page chart “Data Security Legislation in the 109th Congress.”***

## Data Security Legislation in the 109<sup>th</sup> Congress:

As of November 1, 2006

Bill & Cosponsor Info:	Applies to:	Definition of "personal information":	Mandated Security Program:	Consumer Notification Trigger:	Preempts State Laws:	Possible Impact on REALTORS®
<p>S. 1789 – “Personal Data Privacy &amp; Security Act” Intro: 9/29/05</p> <p>Arlen Specter (R-PA) 3 Cosponsors (Bipartisan Support)</p> <p>Approved by the House Judiciary Committee</p>	<p>Businesses that collect, access, transmit, use, store, dispose of, or collect sensitive personally identifiable information.</p> <p><b>*Broad Definition</b></p>	<p><b>SENSITIVE PERSONALLY IDENTIFIABLE INFORMATION-</b> The term `sensitive personally identifiable information' means any information or compilation of information, in electronic or digital form that includes--</p> <p>(A) an individual's first and last name or first initial and last name in combination with any 1 of the following data elements:</p> <p>(i) A non-truncated social security number, driver's license number, passport number, or alien registration number.</p> <p>(ii) Any 2 of the following:</p> <p>(I) Home address or telephone number.</p> <p>(II) Mother's maiden name, if identified as such.</p> <p>(III) Month, day, and year of birth.</p> <p>(iii) Unique biometric data such as a finger print, voice print, a retina or iris image, or any other unique physical representation.</p> <p>(iv) A unique account identifier, electronic identification number, user name, or routing code in combination with any associated security code, access code, or password that is required for an individual to obtain money, goods, services or any other thing of value; or</p> <p>(B) a financial account number or credit or debit card number in combination with any security code, access code or password that is required for an individual to obtain money, goods, services or any other thing of value.</p>	<p>Requires businesses engaged in interstate commerce that involves collecting, accessing, transmitting, using, storing, or disposing of sensitive personally identifiable information in electronic or digital form on 10,000 or more U.S. persons to implement a data privacy and security program.</p> <p>Consumer reporters must protect the security and confidentiality of sensitive consumer financial account or identity information related to any consumer that is maintained, serviced, or communicated by or on behalf of such consumer reporter.</p>	<p>When consumers' personal information is reasonably believed to have been accessed or acquired.</p> <p>*10,000 or more – Highest trigger of any pending bills.</p> <p>Could act as small business exception.</p>	<p>Yes</p>	<p>REALTORS® &amp; Firms:</p> <ul style="list-style-type: none"> <li>-Potential impact/costs for security program for those REALTORS® and large firms with databases of more than 10,000 individuals located in multiple states</li> <li>-Markets near state lines</li> <li>-Members involved in resort property transactions</li> </ul> <p>REALTORS® associations:</p> <ul style="list-style-type: none"> <li>- Potential impact/costs for security programs for large associations who have databases with more than 10,000 individuals covering members in multiple states</li> </ul>
<p>S. 1408 – “ID Theft Protection Act” Intro: 7/14/05</p> <p>Gordon Smith (R-OR) 7 Cosponsors (Bipartisan Support)</p> <p>Approved by the Senate Commerce Committee</p>	<p>Requires any commercial entity, and any charitable, educational, or nonprofit organization, that acquires, maintains, or utilizes sensitive personal information to develop and implement a security program.</p> <p><b>*Broad Definition</b></p>	<p><b>SENSITIVE PERSONAL INFORMATION-</b></p> <p>(A) IN GENERAL- `sensitive personal information' means an individual's name, address, or telephone number combined with 1 or more of the following data elements related to that individual:</p> <p>(i) Social security number, taxpayer identification number, or an employer identification number that is the same as or is derived from the social security number of that individual.</p> <p>(ii) Financial account number, or credit card or debit card number of such individual, combined with any required security code, access code, or password that would permit access to such individual's account.</p> <p>(iii) State driver's license identification number or State resident identification number.</p>	<p>Must have security program when there is a reasonable risk of identity theft to one or more individuals.</p>	<p>When there is a reasonable risk of ID Theft to one or more individuals.</p> <p>*Must affect more than 1,000 individuals to be reported to FTC</p> <p>*Enables Consumers to place security freezes on their credit report</p> <p>*Covered entities can not solicit SSN</p> <p>* No small business exception provision</p>	<p>Yes</p>	<p>REALTORS® &amp; Firms:</p> <ul style="list-style-type: none"> <li>- Potential impact/costs for REALTOR® or REALTORS® firms with databases larger than 1,000 individuals</li> </ul> <p>REALTORS® associations:</p> <ul style="list-style-type: none"> <li>- Potential impact/costs for REALTOR® or REALTORS® firms with databases larger than 1,000 individuals</li> </ul>

Bill & Cosponsor Info:	Applies to:	Definition of "personal information":	Mandated Security Program:	Consumer Notification Trigger:	Preempts State Laws:	Possible Impact on REALTORS®
<p>H.R. 3997 – “Financial Data Protection Act” Intro: 10/6/05</p> <p>Steve LaTourette (R-OH) 22 Cosponsors (Bipartisan Support)</p> <p>Approved by House Financial Services Committee</p>	<p>Consumer Reporters – any consumer reporting agency, financial institution, or person: (1) which, for monetary fees, dues, ...regularly engages in the practice of assembling or evaluating consumer information for the purpose of furnishing consumer reports to third parties, of providing or collecting payment for or marketing products and services, or for employment purposes; and (2) which uses any means or facility of interstate commerce.</p>	<p><b>SENSITIVE FINANCIAL ACCOUNT INFORMATION-</b> The term `sensitive financial account information' means a financial account number of a consumer, such as a credit card number or debit card number, in combination with any security code, access code, biometric code, password, or other personal identification information that would allow access to the financial account.</p> <p><b>SENSITIVE FINANCIAL IDENTITY INFORMATION-</b> The term `sensitive financial identity information' means the first and last name, the address, or the telephone number of a consumer, in combination with any of the following of the consumer: (A) Social Security number. (B) Driver's license number or equivalent State identification number. (C) Taxpayer identification number.</p>	<p>Consumer reporters must protect the security and confidentiality of sensitive consumer financial account or identity information related to any consumer that is maintained, services, or communicated by or on behalf of such consumer reporter.</p> <p>*Legislation is geared towards data brokers/consumer reporters, but because of broad definition this could be applied to other business entities without major obstacles.</p>	<p>If the breached information is reasonably likely to result in “harm or inconvenience” to the consumer.</p> <p>*Has encryption clause</p> <p>*Treats paper and electronic files the same</p> <p>*No small business exception provision</p>	<p>Yes</p>	<p>REALTORS® &amp; Firms: -Would likely largely exclude REALTORS® and REALTORS® firms</p> <p>REALTORS® associations: -Would likely largely exclude REALTOR® associations</p>
<p>H.R. 4127 – “Data Accountability &amp; Trust Act” Intro: 10/25/05</p> <p>Cliff Stearns (R-FL) 15 Cosponsors (Bipartisan Support)</p> <p>Approved by House Energy &amp; Commerce Committee</p>	<p>Information brokers and personas engaged in interstate commerce that own or possess data in electronic form.</p>	<p><b>PERSONAL INFORMATION-</b> (A) DEFINITION- The term `personal information' means an individual's first and last name in combination with any 1 or more of the following data elements for that individual: (i) Social Security number. (ii) Driver's license number or other State identification number. (iii) Financial account number, or credit or debit card number, and any required security code, access code, or password that is necessary to permit access to an individual's financial account. (B) MODIFIED DEFINITION BY RULEMAKING- The FTC may, by rule, modify the definition of `personal information' under subparagraph (A) to the extent that such modification is necessary to accommodate changes in technology or practices, will not unreasonably impede interstate commerce, and will accomplish the purposes of this Act.</p>	<p>Must protect electronic personal information.</p> <p>Information brokers would be required to submit their security policies to the FTC.</p> <p>FTC would promulgate regulations on security program requirements.</p>	<p>When a company reasonably determines that, a security breach poses a reasonable risk of ID theft, fraud, or other unlawful conduct.</p> <p>*Has encryption clause</p> <p>*No small business exception provision</p>	<p>Yes</p>	<p>REALTORS® &amp; Firms: - Potential impact/costs for security programs for REALTORS and firms with clients in multiple states. -Markets near state lines -Members involved in resort property transactions</p> <p>REALTORS® associations: Potential impact/costs for security programs for associations which have databases covering members in multiple states.</p>