SUBJECT: Notifying individuals of unauthorized access to personal information

COMMITTEE: Financial Institutions — committee substitute recommended

VOTE: 6 ayes — Solomons, McCall, Chavez, Flynn, Guillen, Orr

0 nays

1 absent — Riddle

WITNESSES: For — Luke Metzger, Texas Public Interest Research Group; (*Registered, but did not testify:* Brenda Nation, American Council of Life Insurers)

Against — None

On — Rachel Dennis, Texas Bankers Association; Karen Neeley, Independent Bankers Association of Texas; Brad Schuelke, Texas Attorney General; Matt Wall, Texas Hospital Association

DIGEST: CSHB 1682 would require a person who owned or leased computerized personal identifying information to notify individuals promptly in writing or by e-mail if their unencrypted personal information might have been obtained by an unauthorized person.

Personal identifying information would include an individual's name and social security number, driver's license number, or account number and password. It would not include publicly available information.

If a person discovered a security breach, the owner or manager of the information and any service provider would be required to comply with law enforcement actions. The owner or manager could take into account any law enforcement request or measures needed to determine the scope of the breach when notifying individuals of the breach.

If notifying by e-mail, the company would be required to comply with federal regulations about contacting individuals by e-mail, including requiring consent. If the cost of notification was greater than $250,000, it involved more than 500,000 people, or the company did not have full contact information, then notification could be by e-mail without consent

as long as the company also posted a statement on the company's Web site and notified the media of the breach. Breaches that involved more than 1,000 people also would require the company to notify each nationwide consumer reporting agency.

A violation of the notification requirements would constitute a deceptive trade practice, in addition to any other available remedy, and could be the basis for legal action.

The bill would take effect September 1, 2005.

SUPPORTERS SAY:

Companies compile databases that contain very sensitive personal information, and when they are compromised, companies sometimes do not alert their customers that their personal information may have fallen into the wrong hands. Individuals can take action to protect their bank accounts, credit rating, and identity if they learn quickly that their personal information may have fallen into the wrong hands.

Self-regulation of the industry has not worked. Some companies say that their security policies cover information breaches, but recent examples show that the problem is far too widespread to rely on individual company policies. For example, in 2002, more than 55,000 records were accessed at the University of Texas, and two months ago, 32,000 records were taken from LexisNexis. In Congressional testimony, companies have admitted that they have chosen not to notify customers of security breaches. Individuals should have the protection of a single, consistently applied, statutorily required notification process in case their information should ever be taken.

Consumers, not companies, should decide what to do if their information has been compromised. Consumers may ignore notification, just as many ignore product safety recalls, but they still should receive the information.

OPPONENTS SAY:

Requiring companies to disclose every possible breach of computer security — even those where identity theft is unlikely — could result in consumer fatigue. Receiving notification without contextual explanation of exactly what type of information was taken would be of little practical use to consumers. Also, consumers should take precautions when they give out their sensitive personal information, not just after they learn it may have been stolen.

OTHER OPPONENTS SAY:

Texas should let federal law take the lead on this issue. Already, the Health Insurance Portability and Accountability Act (HIPAA) contains provisions protecting consumers from unauthorized access to medical records, and Congress is contemplating legislation to address other personal records.

NOTES:

The committee substitute differs from the original bill in that it would require prompt notification, exempt good faith access to information, require notification of consumer reporting agencies of certain breaches, and not include a civil penalty.