

THE COMMITTEE ON CONSUMER PROTECTION APPROVES REP. STRAUS' BILL ON IDENTITY THEFT.

BOSTON, MA – Rep. Bill Straus (D.-Mattapoisett) announced today that the Committee on Consumer Protection voted favorably to release H. 2797, an Act Relative to The Protection of Personal Information. The bill is scheduled to be acted on by the House of Representatives in a formal session.

The committee vote reflects the work done by the sub-committee on Identity Theft co-chaired by Rep. Straus and Senator Jarrett Barrios (D.-Cambridge). “I am pleased that the Committee acted favorably on my bill and the additions worked on by the sub-committee” said Rep. Straus.

Included in this bill are protections for people in the Commonwealth to help guard against ID Theft, procedures for business and government to follow if personal information is inadvertently released or compromised, as well as new requirements to keep personal information safe and secure. There are four major provisions of the bill: File Freeze, Social Security Number Protection, Breach and Notification, and a revision of the Commonwealth’s Document Disposal regulations.

File Freeze/Credit Freeze:

A truly pro-active component of this identity theft bill embraces a process known as “File-Freeze,” which allows consumers to freeze their credit. This permits the consumer to take an active role in protecting themselves against identity theft by ensuring that no credit is granted in their name. This action will prohibit Consumer Credit Reporting Agencies from releasing a credit report or any other personal information, without the authorization of the consumer, thus ensuring that no new credit may be opened in that person’s name. A “File-Freeze” can be used by all people in the Commonwealth. The bill also directs the credit reporting companies to set up a business practice to allow consumers to unfreeze or thaw their credit history.

Social Security Number Protection:

Included in this legislation are Social Security Number Protection provisions aimed at protecting what is considered to be our most important government identifier. We require that no entity doing business in Massachusetts will require a resident of the Commonwealth to provide his social security number in any manner that would be compromising to the resident. The bill makes it illegal to profit from the sale of a person’s SSN, and sets up regulations that require any computerized transmission of a SSN to be encrypted. The bill prohibits the public release of a SSN without authorization and requires all public documents to have the SSN redacted before documents are made public.

Another major component of the identity theft bill clearly states what comprises a security breach. It also creates a “trigger” requiring the notification of affected parties. Generally, data receivers (any company or entity that holds sensitive data) will be required to notify those whose personal information has been breached when there is a theft of misuse is likely. The bill outlines the procedure for notification and steps that businesses and government need to take to inform affected parties of a data breach.

Finally, any person, business or employee found to be in possession of an illegal “scanning device” will be found to be in violation of the breach of security clause and will be subject to prosecution.

Revision of Commonwealth’s Document Disposal Regulations:

The identity theft bill also details more specific guidelines and procedures for business and government to follow with regard to the proper control of personal information or sensitive data. The purpose of this section is to ensure that personal information contained in documents in the possession of either private business or a government entity is protected. This section of the bill goes on to re-define the regulations currently in place regarding the proper method and procedure for the destruction of documents containing personal information to ensure their identity remains uncompromised.