Testimony Submitted to the Judiciary Committee
On:
Raised Bill Number 671 AN ACT CONCERNING IDENTITY THEFT

Submitted By:
STEVEN BEARAK
Chief Executive Officer
Identity Force

Public Hearing Date: March 14, 2008

Senator McDonald, Representative Lawlor and members of the Judiciary Committee, I appreciate the opportunity to provide testimony to you today regarding this important policy initiative.

My name is Steven Bearak, and I am the CEO of Identity Force, one of the nation's largest identity theft protection companies for consumers and businesses. Identity Force is one of only three companies selected by the U.S. government to provide identity theft services to all federal agencies.

I would like to take this opportunity to applaud your efforts to protect Connecticut citizens from the most prevalent crime in the nation – Identity Theft.

I would also like to take this opportunity to make a few points that relate to Raised Bill Number 671.

First, proper response to data breaches is vital to stopping identity theft.

Data breaches involving the loss or disclosure of personal identifying information can and do lead to identity theft. Last year, over 8.1 million Americans were victims of identity theft and fraud. And last year there were hundreds of publicly-known data breaches (and likely thousands of concealed breaches) that released information on nearly 100 million citizens.

In today's digital world, numbers hold the key to our financial and personal information. Social Security Numbers, Credit Card Numbers, Drivers License Numbers, Health Insurance Numbers, Passport Numbers, Bank Account Numbers and the list goes on. When even one of these numbers is in the wrong hands it can, and does, spell disaster.

When this information is compromised, a comprehensive, well-planned response isn't just the best thing to do – it is the right thing to do.

Second, proper response to a data breach is not credit monitoring.

Credit monitoring alone does nothing more than inform an individual that his or her identity has been stolen. It does not prevent identity theft or fraud. A government agency or business that has somehow released an individual's personal identifying information should be responsible for protecting that citizen from harm.

Third, true protection should be extended to everyone who is placed at heightened risk.

Waiting for thieves to successfully steal a person's money, credit or identity is not an effective solution to a data breach, nor is it, in my opinion, an adequate policy for businesses or governments to follow.

A best-practices and successful approach to identity protection after a data breach should include four basic elements: protection, detection, restoration and reimbursement.

Proactive **protection** of a person's identity includes the aggressive monitoring of cyberspace for the personal identifying information that was compromised. This is one of the most vital components of identity theft protection. Stopping theft and fraud before it can occur not only saves money, it eliminates worry and provides confidence to the individuals affected by data breaches.

Ongoing **detection** through monitoring of credit reports, and the issuance of immediate alerts to any changes in credit reports, including applications for credit in a person's name is also essential.

Identity **restoration** services should also be provided to help identity theft victims recovery their identities and restore their credit, repair damage to their health records, employment records, tax records and other parts of their lives and histories that have been attacked.

Finally, victims should be **reimbursed** for out-of-pocket costs and lost time from work due to identity theft. Typically, this reimbursement can be handled by providing low-cost identity theft insurance.

These four tenets – protection, detection, restoration and reimbursement – are the foundation of real identity theft prevention. Programs that don't provide these elements will, in the end, fail the very people placed at risk by the data breach.

As part of my written testimony today you will see that we have provided some simple wording changes to Bill 671 for you to consider. These recommendations include adding proactive monitoring of the personal identifying information that is lost or disclosed in a data breach. We believe this would, if adopted by the Committee, bring the State of Connecticut's efforts to protect its citizens from identity theft to a new level.

Thank you very much for allowing me to testify today.

Sincerely,

Steven Bearak
CEO
Identity Force