July 18, 2006

Testimony of Congresswoman Darlene Hooley (OR-5)

Before the House Committee on Veterans Affairs

Legislative Hearing on Veterans Identity and Credit Protection Legislation

Good morning and thank you, Chairman Buyer and Ranking Member Filner for the opportunity to appear before the Committee. As one of millions of former credit card fraud victims and as a member of the House Financial Services Committee I have long had a strong interest in protecting consumers from potential ID theft threats and financial crimes.

Identity theft represents a fundamental threat to e-commerce, to our overall economy and to our Homeland Security. No longer are we facing just hobbyist hackers looking to create a nuisance. Increasingly these attacks are driven by skilled criminals and ID theft has become big business.

For the past six years, I've worked in the Financial Services Committee to protect consumers from the threat of ID theft. We've made significant progress in the recent past, including the signing into law of the Fair and Accurate Credit Transactions Act, or the FACT Act, in 2003. That bill, which I was proud to co-author with Congressman LaTourette, provided consumers with landmark new protections, including the right to free annual credit reports and the right to place a "red flag" fraud alert on their credit reports.

Last February, after data security breaches at data brokers Choice Point and Lexis Nexis, I began working on legislation to prevent future data breaches, to provide meaningful notification when consumers are placed at risk of harm by a security breach, and to provide consumers with additional protections when they are placed at risk of ID theft.

The need for such legislation was made crystal clear by the massive data security breach suffered by the VA in May. The details of that breach, which have been highlighted many times before this Committee, underscore the glaring weaknesses in data security policies and procedures at not only the VA, but throughout government agencies and the private sector.

Any data security bill passed by Congress must include a number of key ingredients to be effective.

First, it must mandate data security safeguards and require all businesses and government entities that handle sensitive personal financial information to have robust data security policies and procedures in place. Currently, many businesses and most government agencies are not required to employ such protections, leaving consumers at risk. Mandating protection of sensitive information is the first step in protecting consumers.

Second, legislation must mandate that all businesses and government entities immediately conduct an investigation upon learning that a breach of security might have occurred. That investigation should determine the information involved, whether or not the information is useable, and determine the likelihood that the information has been or will be misused.

Third, legislation should require that upon discovering a breach, the business or government entity notify the Secret Service, their functional regulator, each of the credit reporting agencies, and any third party who must take steps to protect consumers from resulting fraud or identity theft.

Fourth, legislation should include system restoration requirements that require any business or government entity to repair any breach and restore the security and confidentiality of the sensitive financial personal information and to make improvements to its data security policies and procedures.

Finally, legislation should require a meaningful consumer notice anytime a consumer is at risk of account fraud or identity theft. That notice should contain vital information to aid the consumer in protecting themselves from any harm that might result. In addition that notice should provide consumers who are put at risk of ID theft with opportunity to sign up for free of charge credit monitoring services.

Legislation I've coauthored, H.R. 3997, the Financial Data Protection Act, would accomplish exactly that.

However, the breach suffered by the VA, highlighted a few shortcomings of that legislation as it was passed out of the Financial Services Committee. In order to address those shortcomings, I introduced legislation shortly after the massive VA breach that would supplement H.R. 3997.

In the event of a data breach, H.R. 5487, the Veterans' ID Theft Protection Act of 2006, would:

- Authorize funding as necessary to the Secretary of Veterans Affairs to provide credit monitoring as required; and
- Make certain the VA has all necessary negotiating powers to secure the best possible price for the credit monitoring services.

In conclusion, Chairman Buyer and Ranking Member Filner, I would simply state that now is the time to act. The need for federal action on data security is clear and we should not wait for the next catastrophic breach to prod us to action.

Again, I thank you for the opportunity to testify before the Committee today and look forward to working with each of it's members in passing common-sense data security legislation.