

How Delaware veterans can protect themselves in the wake of the data breach at the VA -- May 2006

By: Congressman Mike Castle

On Monday, May 22, 2006 there was an announcement by the Department of Veterans Affairs (VA) that there had been a data security breach. An electronic data file, containing the names, birth dates and Social Security numbers of as many as 26.5 million veterans, was stolen from the home of an employee of the Department on May 3, the data file. As a result, there is of course a need to be cautious if you are a veteran, but no need to panic because at this time, there is no evidence that any of the missing data has been used harmfully. The VA has alerted all veterans to be extra vigilant about their credit reports, therefore, I would like to outline some places to turn and things to be looking for as the investigation continues on this breach.

The Washington Post reported that affected veterans include anyone discharged after 1975 and some of their spouses, as well as some veterans discharged before then who submitted a claim for VA benefits. Because the affected veterans could be vulnerable to credit card fraud if the burglars realize the value of the data, the Department is warning all veterans to be extra attentive to their bank statements, credit card statements and any statements relating to recent financial transactions. Under a new Federal law, you have the right to receive a free copy of your credit report once every 12 months from each of the three nationwide consumer reporting companies. To request your free annual report under that law, you must go to <http://www.freecreditreport.com/ACRRredirect.aspx?SiteVersionID=461&SiteID=100133&sc=666977&bcd=>. The VA also encourages veterans to visit their website at <http://www.firstgov.gov/> or call 1-800-FED-INFO (1-800-333-4636) for up-to-date information on the issue.

If you would like to report unusual activity, there are several different courses of action. One option is to contact the fraud department of one of the three major credit bureaus, Equifax, Experian or TransUnion. You can close any account that has been tampered with or opened fraudulently or you can file a police report with local police. Finally, you can file a complaint with the Federal Trade Commission (FTC) by using the FTC's Identity Theft Hotline. You can call that hotline at 1-877-438-4338 or go online to www.consumer.gov/idtheft.

Because this threat represents the biggest unauthorized disclosure of Social Security data in history, the Department of Veterans Affairs is working with the President's Identity Theft Task Force, the Department of Justice and the Federal Trade Commission to investigate the breach and to make sure that it cannot and will not happen again. Some of the preventative measures taken have been directing all VA employees to complete Security Awareness and Privacy Awareness training by June 30, 2006. Additionally, the Department of Veterans Affairs will be conducting an immediate inventory and review of all current positions to ensure that all VA employees have the correct and relevant access to information dependent on their position. Finally, the FBI and the Inspector General are conducting full-scale investigations into the situation.

For my part, I am still working on the Financial Data Protection Act, H.R. 3997 that works to protect consumers against data breaches and strengthens the notification process if a breach does occur. The passage of this key legislation is critical because of occurrences like these and because of the increased access to credit, more product and service price competition and mounting issues related to public safety. Specifically, the legislation attempts to prevent breaches of data, mandates an investigation upon discovery of a breach, provides notice to any victim of a breach, provides financial

fraud mitigation to the consumer and creates additional regulations. My hope is to move forward with this bill, perhaps making changes to include federal agencies and departments in light of this recent breach so that the most comprehensive financial data protection plan is in place.

As always, you can also direct any additional questions, concerns or comments to my office at 302-736-1666 or 302-428-1902. Please remember to be attentive to your financial data, but do not feel the need to do anything drastic in light of these revelations. Be assured that the matter is being addressed and the hope is that in the end, not one veteran will be affected.