STATEMENT OF STUART K. PRATT

CONSUMER DATA INDUSTRY ASSOCIATION

WASHINGTON, D.C.

Oversight Hearing: Department of Veterans Affairs Data Breach

Committee on Veterans' Affairs

United States House of Representatives

Washington, D.C.

Tuesday, May 25, 2006

Chairmen Buyer, Acting Ranking Member Filner, and members of the committee, thank you for this opportunity to appear before you today. For the record, my name is Stuart Pratt and I am president and CEO of the Consumer Data Industry Association.[1] We appreciate this opportunity to discuss the Veterans Administration's loss of sensitive personal information on as many as 26.5 million veterans.

Planning and Coordination

This past weekend, CDIA was contacted by the Federal Trade Commission regarding this breach. We are thankful for the FTC's outreach to us, which allowed the CDIA to liaison with our national credit reporting company members who had to plan for likely heavy call volumes on their toll free numbers and hit rates on their websites. Based on this contact our members' technology teams were alerted in preparation for the announcement on Monday, May 23rd. As part of this very late-stage coordination, our members also voluntarily either adjusted current toll free number menus to include special reference for affected veterans, or implemented entirely new toll free numbers which can be used by veterans to request the placement of a fraud alert on a their credit reports. Once a fraud alert is placed a veteran is then, by law, entitled to order a copy of his or her credit report free of charge. Our members report that subsequent to the announcement by the Veterans Administration and ensuing media coverage that call volumes have been running approximately 170 percent over normal rates.

If we have a criticism of this process it is the fact that our members were not consulted sooner by

[1] CDIA, as we are commonly known, is the international trade association representing over 300 consumer data companies that provide fraud prevention and risk management products, credit and mortgage reports, tenant and

the Veterans Administration (the FTC notified us as soon as they were permitted to do so), though perhaps there are extenuating circumstances of which we are not aware. Had the FTC not notified us, we would not have had any opportunity to plan for the contact volumes our members are now experiencing, which are high, but manageable. Even over the weekend, the FTC was not permitted to release the name of the agency and thus our members could not execute plans to customize toll-free number service until after 11:00 a.m. on Monday, May 23rd. Government agencies should be obligated to coordinate with our members well in advance where they intend to publish advice which includes our members' contact information. This is simply the right step to take so that our members can verify the accuracy of the information and ensure that our systems are prepared for increased in contact volumes. Ultimately this obligation helps us all serve affected consumers.

Recommended Steps for Veterans

Your staff indicated interest in hearing what steps we would recommend that a veteran take in response to the announcement. Our views on the key steps for veterans are no different than the information that the FTC has already compiled. We believe consistency in messages is important at this time to ensure that all veterans empowered to take steps that are appropriate to the risk. Following is the latest FTC advice:[2]

Things to Consider

- Because your Social Security number can be used by ID thieves to open up fraudulent accounts in your name, watch for signs that your personal information has been misused. For example, bills that don't arrive on time, receiving credit cards you didn't apply for,

---

employment screening services, check fraud and verification services, systems for insurance underwriting and also collection services.

[2] See http://www.ftc.gov/veterans

being denied credit or receiving unfavorable terms like high interest rates for no apparent reason, or being contacted by debt collectors or businesses about merchandise or services you didn't buy.

- You can order your free annual credit report. You can order online at **annualcreditreport.com**, or by calling toll free 877-322-8228, or by writing Annual Credit Report Request Service, Box 105281, Atlanta, GA, 30384-5281.

- Once you receive your report, review it for suspicious activity like inquiries from companies you didn't contact, accounts you didn't open, and debt on accounts you cannot explain. Check that other information, like your address, date of birth or employer, is correct.

- Consider placing a fraud alert on your credit file. (Note: You may find it more difficult to obtain new credit while there is a fraud alert on your credit file.)

- To place a fraud alert, call the toll free number of any one of the three nationwide consumer reporting agencies. That agency will inform the other two. This alert can help stop someone from opening new credit accounts in your name. An initial fraud alert stays on your credit report for 90 days. After 90 days, if you want to extend the fraud alert for an additional 90 days, you may do so.

  TransUnion: 800-680-7289; **www.transunion.com**
  Equifax: 877-576-5734; **www.equifax.com**
  Experian: 888-397-3742; **www.experian.com**

- When you place a fraud alert with one of these three companies, you'll receive information about ordering one free credit report from each of the companies. Many people wait about a month from when the information was stolen to order their report because suspicious activity may not appear right away.

- If you learn that your information has been misused, file a complaint with the police, and with the Federal Trade Commission at **ftc.gov/idtheft** or 877 ID THEFT. The FTC website also has step-by-step instructions on other measures to take, including an ID Theft Affidavit that consumers can use when disputing unauthorized accounts.

For more information visit:

- Identity Theft Tips from the Federal Trade Commission
  www.ftc.gov/idtheft

- The U.S.Government's Official Web Portal
  www.FirstGov.gov/veteransinfo

- Department of Veterans Affairs
  www.va.gov

We would only add emphasis to the FTC's point that veterans need only call one national credit reporting company to place a fraud alert since our members exchange fraud alert requests. Further, upon placement of fraud alerts veterans are entitled to a free copy of their credit report and will receive instructions for how to order this. Some veterans might be confused about whether or not they need to use **www.AnnualCreditReport.com** to order their free report resulting from placement of the fraud alert, and in this case, the answer is no, they should follow the instructions provided by the national credit reporting company which will be part of a written confirmation that the fraud alert has been placed.

CDIA Position on Data Security and Notification of Consumers

As demonstrated by this breach, data security and the need to notify consumers (including our nation's veterans) where significant risk of harm exists is essential. The following statement delivered during our testimony before the Senate Banking Committee on September 22, 2005 continues to reflect our position on protecting sensitive data about consumers:

> *"The discussion of safeguarding sensitive personal information and notifying consumers when there is a substantial risk of identity theft has expanded beyond the boundaries of financial institutions. It is our view that rational and effective national standards should be enacted both for information security and consumer notification as it applies to sensitive personal information, regardless of whether the person is a 'financial institution.'"*

As this committee knows, there are a number of House and Senate committees that are focused on developing uniform national standards for ensuring the protection of sensitive personal information. We believe that enactment of national standards will ensure that sensitive personal

information is protected by all who possess it, including federal and state governmental agencies. New nationwide safeguards regulations authored by the Federal Trade Commission will compel all to deploy physical and technical strategies for the protection of sensitive information about consumers.

Ultimately national standards for the safeguarding of sensitive personal information will address consumer concerns and perceptions, including those of veterans who rightly expect that their information will be secured. These are all good public policy results and CDIA remains committed to a constructive dialogue as various bills move through the House and Senate.

Conclusion:

As we head into a Memorial Day weekend, we must redouble our efforts to pass strong and effective national law that will require all to secure personal information properly and to notify consumers when there is a significant risk of identity theft due to a breach of such information. We should do no less for our veterans who have served us all.

Thank you for this opportunity to testify and I would be happy to answer any questions.