Written Testimony of ID Analytics Corporation

Oversight Hearing on the Veterans Affairs Data Breach

Washington D.C.
June 22, 2006

Chairman Buyer, Ranking Member Evans, and distinguished members of the Committee:

Thank you for inviting ID Analytics to testify on ways to help victims of the recent Veterans Affairs data breach.

My name is Mike Cook. I am a Co-Founder of ID Analytics, a San Diego-based company focused exclusively on stopping identity fraud. I have worked in the field of credit risk and fraud prevention for 20 years

ID Analytics helps stop identity fraud through our ID Network, a real-time identity fraud prevention system formed through a consortium of leading companies dedicated to protecting their customers from identity fraud. Our ID Network gathers information from applications for credit, change of address, and other identity risk information from companies including half of the top ten US banks, almost all major wireless carriers, and a leading retail credit card issuer. Hundreds of times each day, our technology helps stop fraudsters from obtaining credit, services and merchandise in innocent consumer's names. We think it's important to make you aware that ID Analytics does not market or sell the data we collect in the ID Network for any purpose, to anyone.

I am here today because ID Analytics has unique expertise and knowledge of data breaches and their risks. To date, we are the only public or private entity that has studied the harm resulting from actual data breaches. Should any Committee member have interest, I would be happy to provide a copy of our White Paper analyzing the harm from

four actual, well publicized data breaches involving more than 500,000 breached consumer identities.

I would first like to put this breach into context. At this point, no one knows the scope of risk veterans are facing. The most dangerous data breaches are targeted thefts, where the thief committed the breach solely for the purpose of taking consumer data. In this case, the purpose of the theft is unclear. Was the thief targeting a laptop or the data held on it? I don't believe we know that answer today.

If the data is misused, we can expect it to be misused in the following ways:

- It is likely the fraudsters will mainly attack the credit card industry. Stolen identities are an asset, and sophisticated fraudsters can get the best rate of return by fraudulently obtaining credit cards and then making fenceable purchases.
- Because the file contains so many identities, it is likely that the fraudsters will use the stolen identities once or twice and never again to increase their approval rate. Low use rates of individual veteran identities will make detection more difficult for the lending community.
- Again, *if* the data is misused, sophisticated fraudsters will spread the misuse of the identities across differing locations within a city or even across different states to avoid detection.

The worst case scenario is that the Veterans file finds its way to a public distribution source, such as the Internet. If this happens, the stolen identities will lose their connection to the VA data breach and groups of

fraudsters might actively trade that data among the fraud community. Subsequently, more people might have access and could misuse those identities on a grander scale. We know from additional research conducted this year that the misuse rate of data traded on the Internet can climb substantially and exceed the average rate of identity theft of 1.5%.

Some consumer advocates estimate that the value of a stolen identity ranges from $25 to $75 depending on the available personal information associated with that identity. So, because of the value of the data itself, wide distribution should be a concern, and should drive a real sense of urgency to try to recover the stolen data back as fast as possible.

So, what can the VA do now?

Over the course of the last year, ID Analytics has developed breach monitoring technology. With this technology, the VA can answer three essential questions about the data breach

1) Is the breached data being misused by fraudsters today?
2) If it is being misused, can we identify the specific veterans harmed by this misuse and provide them with additional victim assistance?
3) If the breached file is being misused, at what locations are those breached consumer identities being misused so that law enforcement can stop the misuse and potentially acquire back the breached data file?

How does this technology work? Simply put, when thieves use a breach file, they leave tracks. In order to obtain credit or other goods in a

veteran's name, a fraudster would have to manipulate that veteran's identity information on a new account application. For instance, if a fraudster applies for a credit card in a veteran's name, the fraudster needs to change the address (so he or she can collect the new credit card from the bank). The fraudster will change the veteran's phone number for personal and employment verification purposes. He or she may use these same addresses and phone numbers to commit identity theft against other identities that were part of the same breach. Our ID Network, which receives hundreds of thousands of applications and other identity risk events per day, can identify these types of anomalous changes and relationships across a breached file, regardless of the size of the breached file.

We believe this technology can be significant to the Department of Veterans Affairs for the following reasons:

- It can help identify any organized misuse of the personal data that has happened so far;
- The analysis can quickly identify veterans who may have been victimized so that additional victim assistance can be expedited to them;
- It can actively monitor the file for possible misuse;
- This technology can help provide law enforcement a way to identify those individuals who have either stolen the file or have misused it to commit identity theft, to stop further misuse and to recover the lost file;
- The analysis can help determine if the file is in use by more than one individual (or one cohesive group);

And finally, breach monitoring provides a deterrent effect once publicly announced. Thieves should be aware that if they try to misuse any data from the VA data breach, they do so at their own peril.

Thank you again, Mr. Chairman for the opportunity to present this testimony.