Uploaded to VFC Website

November 2012

This Document has been provided to you courtesy of Veterans-For-Change!

Feel free to pass to any veteran who might be able to use this information!

For thousands more files like this and hundreds of links to useful information, and hundreds of "Frequently Asked Questions, please go to:

Veterans-For-Change

Veterans-For-Change is a 501(c)(3) Non-Profit Corporation
Tax ID #27-3820181

If Veteran's don't help Veteran's, who will?

We appreciate all donations to continue to provide information and services to Veterans and their families.

https://www.paypal.com/cgi-bin/webscr?cmd=_s-xclick&hosted_button_id=WGT2M5UTB9A78

Note: VFC is not liable for source information in this document, it is merely provided as a courtesy to our members.

Identity Theft Alert: Veteran Data Theft

By Credit.com

On May 23, the Veterans Affairs Department announced that an employee laptop containing 26.5 million veteran records was stolen. This computer contained sensitive records, including Social Security numbers, on all veterans who were discharged since 1975 and some of their spouses. Veteran medical and financial information was not included, but there may have been disability data on the laptop. More information about this crime is available at FirstGov.gov.

In past data theft cases, approximately 2% of the people who had their information stolen eventually faced actual identity theft crimes. In this case, 2% equals a whopping 520,000 veterans. Due to the extraordinary extent of this crime, it remains be to seen how many victims will emerge. No incidents of identity theft related to this crime have been reported yet but the data is a potential goldmine for identity thieves. It is possible that the stolen data will not be misused for weeks, months or even years.

Veterans should take a few simple precautions now to protect their credit from identity theft crimes related to this data theft. Credit.com recommends the following five steps:

1. Place a fraud alert on your credit reports

Call one of the three national credit bureaus to have a 90-day fraud alert added to all three of your credit reports. This fraud alert notifies businesses that your identity may be compromised and could prevent new accounts from being opened in your name. You will also be sent a free copy of your credit report by mail when you place this fraud alert request:

Equifax
1-800-525-6285
www.equifax.com
P.O. Box 740241
Atlanta, GA 30374

Experian
1-888-EXPERIAN
www.experian.com
P.O. Box 9532
Allen, TX 75013

TransUnion
1-800-680-7289
www.transunion.com
Fraud Victim Assistance Dept.
P.O. Box 6790
Fullerton, CA 92834

2. Order your free credit reports

Credit.com recommends that you check your credit reports online while waiting for the mailed reports to arrive. There are two free ways to check your credit reports online. The first is through AnnualCreditReport.com, the credit bureau's free disclosure site as mandated by the Fair and Accurate Credit Transaction Act. Credit.com has instructions for using this site.

If you have already ordered your free credit report disclosures for the year, there is another way to obtain free credit reports. You can order a free credit report online from Experian and TransUnion if you suspect that you may be a victim of identity theft. Equifax will only send these identity theft disclosure reports by mail. Request your Equifax report by calling 800-685-1111.

3. Look for signs of theft

Once you have obtained your credit reports, review each file for signs of identity theft. Look for the following:

- Address changes
- Name changes
- New unauthorized accounts
- Usual balance or payment records
- Inaccurate public records (liens, judgments, collections)
- Unauthorized inquiries (applications for credit)

If you do spot signs of identity theft on your credit report, contact your creditors immediately to report the crime and reverse the charges. You should also file a police report and complete an identity theft affidavit with the Federal Trade Commission. Ask the credit bureaus to extend your 90-day alert to a 7-year fraud alert using your police report. The FTC has more instructions for resolving specific identity theft crimes.

4. Consider a file freeze

In some states, it is possible to "lock" your credit report data from all access. With this freeze, you will have to grant creditors specific permission to check your credit each time that you want to open a new account. These freezes can also impact insurance, job, apartment and cell phone applications as well as your ability to check your own credit reports online. A freeze is the best protection available against unauthorized use of your credit data.

Security freezes are currently available to residents of California, Connecticut, Illinois, Louisiana, Maine, Nevada, New Jersey, North Carolina, Texas, Vermont and Washington. Colorado, Kentucky and South Dakota will also allow file freezes after July 1, 2006.

However, the costs and requirements for these freezes vary by state. Click here to review the complete requirements. If you qualify, contact the credit bureaus at the numbers listed in step 1 to request a file freeze.

5. Investigate the free offers

Credit and fraud monitoring services can be a great way to track your credit data and be alerted of suspicious changes. These services automatically scan your personal data and send you email alerts when items change.

Normally, these products range from about $10/month to $200/year. Several different companies are offering free or discounted services to veterans impacted by this data theft. Here are few of the offers available:

Equifax – 50% off the three varieties of credit monitoring programs offered by Equifax through June 30th.

Intersections – Six months of free Identity Guard Fraud Protection. A $4.95 processing fee applies.

Intelius – One free year of IDWatch for a discounted price of $19.95.

Have a question about identity theft or these instructions for veterans? Contact us or send an email to tidbits@credit.com. We'd be glad to help.