

**The Veteran's
Information Guide To
Combating Identity Theft**

What Veteran's Should
Understand About the Government's
Mishandling of Your Personal & Private
Information
And
What You Should Do NOW

July 30, 2006

Preface

About two months ago, America's veterans were shocked to learn their personal records had been removed from the Headquarters, Veterans Administration in Washington D.C., and taken to the residence of an employee, who subsequently reported the data stolen during a home burglary.

Stunned VA officials claimed they knew nothing of the occurrence for nearly several weeks; later we learned some senior officials kept the data loss a secret and multiple congressional hearings disclosed what could only be described as inept and bumbling security policies at the agency responsible for veteran's health care.

Numerous stories were published about the events but ever since the "miraculous" recovery of the missing data, the story has fallen off the radar of America's national media. After all, it wasn't their personal records that were mishandled, and they aren't even interested in knowing how the information was recovered! The theft only involved 26 ½ million "other" people.

This paper provides a brief chronology of key events associated with the story but more importantly, does what the VA failed to do. It provides America's veterans some specific and detailed assistance regarding what protective measures they should now be taking since their information was mishandled, and then allegedly stolen.

How many of us will pay the price for the incompetence of government bureaucrats? I don't know. How many of us are already paying the price and don't even know it? Again, I don't know.

What I do know is that veterans must be proactive to protect themselves. Hopefully, this guide offers some direction to those who aren't sure what to do or who to contact.

OVERVIEW

- **BACKGROUND**
- **OBJECTIVES**
- **ACTIONS**
- **ADDITIONAL RELATED INFORMATION**

BACKGROUND

- May 10, 2006, President establishes by Executive Order, Presidential Identity Theft Task Force.¹
 1. Co-chaired by Attorney General and Chairperson, FTC
 2. 13 senior government officials are permanent members
 3. Secretary of the Veterans Administration is a permanent member

- May 22, 2006, VA releases Statement² that an employee, without authorization and in violation of department policy, removed electronic data to his residence which was subsequently stolen.

- FBI & VA Inspector General along with local law enforcement reportedly conducting investigations.

- VA working with members of Congress, the news media, (some) veteran service organizations and other governmental agencies to assist veterans and their families.

- VA to mail out notification letters to affected veterans.

- President's Identity Theft Task Force working with credit bureaus to help insure that veterans receive the free credit report they are entitled to under the law

¹. May 10, 2006, Office of the White House Press Secretary, <http://www.whitehouse.gov> Executive Order: Strengthening Federal Efforts to Protect against Identity Theft

². May 22, 2006, 2 pgs, Department of Veterans Affairs *Statement*

- "Task Force to meet to coordinate comprehensive Federal Response, recommend further ways to protect affected veterans..."
- May 23, 2006 initial media reports³ begin reporting that approximately 26.5 million veterans at risk when official personal data including names, social security numbers and dates of birth allegedly stolen from the home of a VA employee.
 1. Media reports that alleged burglary occurred May 3rd in Maryland & reported to Montgomery County Police Department
 2. Burglary characterized as "random."
 3. Affected veterans initially reported as "anyone discharged after 1975; some of their spouses, some veterans who submitted claims prior to 1975."
 4. "biggest unauthorized disclosure ever of Social Security data..."
 5. Data doesn't contain medical records or financial information but in some cases, disability ratings.
- May 26, 2006, VA Inspector General discloses⁴ that data analyst responsible for taking home stolen electronic data was routinely taking home official information since 2003.
 1. Federal investigators have removed other sensitive VA data the worker was not authorized to have at home.
 2. Veterans Affairs Secretary Jim Nicholson said the stolen information was not encrypted or "scrambled."

³. May 23, 2006, Washington Post article "Personal Data on Veterans is Stolen

⁴. May 26, 2003, Washington Post article, pg 19., "Worker Often took Data Home"

3. (VA Inspector General George J.) Opfer said his office did not learn of the lost data until May 10, and then only through an offhand remark by a VA employee at a routine meeting.
 4. VA Secretary not briefed until May 16th.
 5. FBI not told until May 17th.
- May 30, 2006, first of two Class Action Law Suits filed against VA & named officials.
1. 1st case filed in U.S. District Court, Eastern District of Kentucky, Case Number 06-114-WOB⁵
 2. 2nd case filed in U.S. District Court for the District of Columbia filed by the Vietnam Veterans of America (VVA) and four other veteran organizations against the Department of the VA, Case Number 1: 06CV01038⁶

⁵. May 30, 2006, 13 pg document dated May 30th 2006, U.S. District Court Eastern District of Kentucky.

⁶. June 6, 2006, 16 pg document dated June 6th, 2006, U.S. District Court for the District of Columbia

- May 31, 2006, Marine veteran appointed to 3-month contract to investigate theft of VA data and evaluate VA Information Technology Program⁷
- June 2, 2006, VA Secretary announces⁸ appointment of Rick Romley, new special advisor for information security.
- June 2, 2006, VA deputy secretary resigns⁹
- June 2, 2006, Vets still in dark about details of theft; some states offer "credit freeze."¹⁰
- June 3, 2006, initial disclosures of 50,000 Navy & National Guard active duty personnel also affected by data theft¹¹
- June 7, 2006, Nearly all active duty, Guard and Reserve, 2.2 million personnel, may be affected by data theft¹²
- June 9, 2006, data analyst who took information "dismissed."¹³

7. May 31, 2006, The Arizona Republic, Rick Romley tapped for veterans ID theft case

8. June 2, 2006, The Business Journal of Phoenix, "Romley named Special Advisor to VA Secretary

9. June 2, 2006, Tech Web, VA shake up follows identity theft

10. June 2, 2006, Seattle Post-Intelligencer, Vets Still in Dark About Data Theft

11. June 3, 2006, Associated Press, IDs of Active Personnel on Stolen Laptop

12. June 7, 2006, Associated Press, Data on 2.2M Active Troops

13. June 9, 2006, New York Times, Garden Variety Burglar Suspected in Loss of Data

- June 9, 2006, VA Secretary advises Congress that employee who took data and two supervisors are fired.¹⁴
 1. (VA Secretary) Nicholson told lawmakers VA's information security policies are generally adequate.
 2. He ticked off the steps he's taken to improve data security at VA in the weeks since the data breach. He hired a new special adviser for information security, Richard Romley. He's directed top department leaders to remind managers and staffs to protect sensitive information. He's launched an internal program to beef up data privacy and security procedures. He's compiling an inventory of all positions requiring access to sensitive data. And he's ordered a security review of all laptops,
 3. Asked if he was surprised about the loss of personal information, Clay Johnson, OMB's deputy director for management, told lawmakers the VA incident was the "100-year storm of security breaches."
 4. Rep. Steve Buyer, R-Ind., chairman of the House Veterans' Affairs Committee, said he wants a complete reorganization of the VA information technology system to provide more centralized control.
 5. "We really need to have some safeguards so you simply cannot remove data and take it home with you," Buyer said. "No rules, no organizational structure, is going to stop problems as long as it is possible for someone to walk out the door with data."

¹⁴. June 12, 2006, Federal Times, Beefed-up privacy top concern after VA data loss

- June 21, 2006, VA Secretary announces VA to Provide Free Credit Monitoring. *The following is extracted from the press release:*
- "VA will solicit bids from qualified companies to provide a comprehensive credit monitoring solution. VA will ask these companies to provide expedited proposals and to be prepared to implement them rapidly once they are under contract."
- "After VA hires a credit monitoring company, the Department will send a detailed letter to people whose sensitive personal information may have been included in the stolen data. This letter will explain credit monitoring and how eligible people can enroll or "opt-in" for the services. The Department expects to have the services in place and the letters mailed by mid-August."
- Secretary Nicholson also announced VA is soliciting bids to hire a company that provides data-breach analysis, which will look for possible misuse of the stolen VA data. The analysis would help measure the risk of the data loss, identify suspicious misuse of identity information and expedite full assistance to affected people.
- A new "update" was posted on the USG web site, www.firstgov.gov regarding the VA information loss. The following was extracted on June 21st, 2006:

"What action has been taken against this employee or his supervisor?"

The employee is cooperating fully with the investigation. The employee was initially placed on administrative leave, and VA is implementing procedures necessary to dismiss the employee. Also, the official responsible

for the organization in which this employee served has resigned his position because of the events. (Previous reporting was that this employee was terminated, but now is being reported very differently.) See footnote #13, above.

- June 21, 2006, House Judiciary Committee by voice vote, approved legislation thought to pass the entire House, "compensating veterans who might be victims of identity theft because of the loss of millions of Veterans Affairs Department personnel records."¹⁵
- From May through June, the Senate Veterans Affairs Committee holds hearings with government and private officials regarding privacy issues, Information Technology issues and identity theft issues.
- June 29, 2006:
 1. Secretary of the VA Nicholson announces prior to House Veterans Affairs Committee that "missing" laptop and hard drive were recovered by local law enforcement agencies. The hardware is undergoing forensic investigation to determine if information was copied.
 2. Secretary Nicholson also providing extensive briefing on what other "corrective actions" he has directed to be implemented regarding the handling of veteran's personnel data.

¹⁵. June 22, 2006, "House panel OKs office to compensate vets for ID theft," http://www.govexec.com/story_page.cfm?articleid=34381&dcn=todaysnews

3. One committee member stated that the person responsible for the alleged "loss" was in fact, authorized to remove the information and had permission to do so. (This will be further detailed in the committee hearing, I am sure.)
4. Committee Chairman, Rep Buyer, opened committee hearing by announcing three unrelated security incidents involving "losses" of other veteran related information including alleged loss of over 16,000 legal cases.
5. Baltimore Division, FBI Press Release¹⁶ reported "...A preliminary review of the equipment by computer forensic teams determined that the database remains intact and has not been accessed since it was stolen. A thorough forensic examination is underway, and the results will be shared as soon as possible..."
 - Note: Press release says a "preliminary review" conducted with a "thorough forensic examination underway."
 - Sec Nicholson clearly implied by his surprise disclosure on the Hill that veterans no longer must worry because no one accessed the lost personal data.
 - Clearly, the suggestion veterans don't have to worry was speculative at best, yet this issue has now become "old news," and does not carry the weight as it did when first reported.
 - Secretary Nicholson no longer supportive of VA credit reviews to assist veterans!

¹⁶. June 29, 2006, Baltimore Division, FBI Press Release, 1pg, [.http://baltimore.fbi.gov/pressrel/2006/laptop_062906.htm](http://baltimore.fbi.gov/pressrel/2006/laptop_062906.htm)

6. Unanswered questions to VA mishandling of veteran data. The following questions were not asked by the Senate or House Veterans Affairs Committees and remain unanswered to America's veterans.

- When exactly, was the information originally removed from HQ VA that was subsequently stolen from the employee's residence?
- Who signed the document(s) authorizing the removal of the information?
- Were those who signed the document(s) authorized to do so?
- If the signers of the document(s) were not authorized to do so, why did they do it this time?
 - Did the signer of the document have authority to approve any property removal?
 - Did the signer of the document sign similar documents in the past?
 - What actions have been taken against the (unauthorized) signer of the document(s)?
 - What procedures have been implemented to insure unauthorized personnel no longer sign removal documents?
 - What procedures have been implemented to insure electronic data is removed only under authorized conditions and by authorized authority.
- Why were the initial "reports" of the data removal characterized as "unauthorized," when document(s) existed giving the employee permission to remove the data?
- What type of check and balance system exists (or now exists), to insure

that personnel will obtain proper authorization to remove sensitive information from the VA work site.

- In what format was the information that was removed from the VA work site?
- How many CD-ROMs were utilized to remove the information and were all the original CD-ROMs used to remove the information, recovered?
- How is it known that the exact same CD-ROMs were recovered, and not copies of the original CD-ROMS?
- Where (location), and when was the data transferred from the CD-ROMs to the laptop computer or external hard drive?
- Why weren't the original CD-ROMs returned to the HQ VA work site after the information was transferred to the hardware?
- If information is returned, what procedures are utilized to document the return and verification of the data originally removed from the work site?
- If procedures don't exist, why not, and when will procedures be implemented?
- Regarding the information taken by the employee, what procedures, if any, were utilized to protect the information when it was removed from the VA work site.
- Was the information transferred to official government hardware authorized for use outside the VA work site or was it transferred to personal property?
- Do VA employees, in general, have the "authority" to routinely transfer official US Government information onto personal equipment?

- What measures existed before the incident and now, since the incident, to insure that official USG information is only utilized on official equipment and not on personal equipment?
- Do VA employees continue to use personally owned "thumb drives" and other portable media within the VA to perform "official duties," as described by Secretary Nicholson before Congressional committees?
- If so, what regulations have been established delineating the conditions under which such equipment can be utilized; how information will be accounted for and utilized with such equipment and what procedures will be followed when returning & accounting for such information?
- Regarding the information that was removed from the VA work site and then allegedly stolen from the Maryland residence:
 - Who had access to the information at the residence?
 - Who has been identified as having seen this information before it was allegedly burglarized?
 - How was the information stored at the residence before it was allegedly stolen?
 - Was any of the personal data "copied" on other storage media when it was at the residence?
 - If so, where is this media now and in whose possession was it when it was recovered?
 - Has the ongoing law enforcement investigation regarding this incident disclosed any attempt to "hack" into the hardware at

the residence while VA records were stored on it at the residence?

- What security measures were utilized at the residence while the information was stored on the personal hardware to insure no unauthorized persons "hacked" or "accessed" the information while it was being stored there.
- Specifically, for how long were our personal records stored at the Maryland residence before they were burglarized?
- Specifically, when was the missing hardware "recovered, i.e., how many days after it was stolen from the house was it recovered and where was it when it was recovered?
- Were the original CD-ROMs which were used to remove the personnel information also stolen with the hardware or were they returned to the VA at an earlier date?
- What are the "specifics" with respect to who had access to the hardware and the CD-ROMs after the May 3rd burglary?
 - Who had access to the equipment AND information?
 - Did anyone physically view the information, even if no evidence now exists that they made copies of the information?
 - Have all the involved parties been polygraphed to verify their stories with respect to the recovered hardware and CD-ROMs?
 - What are the circumstances regarding the "recovery" of the missing hardware/information?

- Have all involved personnel executed "sworn statements" pertaining to their roles and participation in receiving, possessing and eventually transferring the stolen hardware/information to law enforcement personnel?
- Are there still identified or unidentified person(s) who've not yet been interviewed regarding the original "burglary" as well as the "recovery?"
- If so, how many people are involved and do leads exist whereby these individuals can be reasonably expected to be interviewed in the near term or the long term?
- How long will it take for the FBI to determine whether the CD-ROMs and hard drives were accessed by unauthorized persons?
- What forensic methods are being utilized by the FBI to determine if unauthorized access occurred?

Author's Comments: The preceding list of questions represents a cursory list of unanswered questions regarding the alleged stolen & recovered hardware & information. Clearly, law enforcement agencies will conduct far more thorough activities than listed above; however, I believe the public has a right to know certain basic facts pertaining to the case that will not compromise the investigation. The above questions represent the kinds of data that could be disclosed to Congressional committees and should be disclosed in the interest of all affected American veterans. This author has provided some of this information to the affected congressional committees; however, I've received no reply from anyone. Failure by the VA to clearly disclose all pertinent facts reflects a disrespectful attitude to all affected veterans

7. July 11, 2006, the VA/OIG publishes it's report entitled "Review of Issues Related to the Loss of VA Information Involving the Loss of Millions of Veterans"
 - Numerous criticisms pertaining to poor security management, oversight, and reporting cited in the 78 page VA/OIG report [
<http://www.va.gov/oig/51/FY2006rpts/VAOIG-06-02238-163.pdf>]
 - "Inadequate department policies, indifference, a lack of urgency," and a general malaise of poor senior leadership were all detailed in the OIG report.
 - "Uncorrected weaknesses" cited.
8. July 20, 2006, VA Secretary reneges at Senate Veterans Affairs Committee hearing on his prior offer to provide credit monitoring for affected veterans.

OBJECTIVES

1. To provide an overview of significant events associated with the public reporting of mishandled and lost personal records associated with 26 ½ million American veterans and family members, including approximately 2.2 million records of the Active Military Force.
2. To Provide an overview of the proactive measures American veterans and their families can take to mitigate unacceptable government complacency and bungling associated with the loss of personal identities and the potential greater impact on personal financial records and reputations.
3. To provide references associated with Identity Theft that American veterans and family members may not be aware of.

ACTIONS

Caveat 1. In the absence of any substantive effort by the U.S. Department of Veterans Affairs to assist America's veterans whose personal information has been grossly mishandled, it is incumbent upon veterans themselves to take timely and effective action to protect their individual financial records, reputations and good names.

Caveat 2. The information contained herein has been derived from public sources and personal experiences. The author of this paper is a military retiree and has been an Identity Theft victim on several past occasions. My personal information has also been mishandled by others, besides the Veterans Administration. I've had bank accounts and credit cards compromised; unknown persons have attempted to open accounts and cash checks in my name and I've had U.S. mail stolen as a result of the actions of others, and fraudulent purchases have been made in my name. All this has occurred in the past five years.

Caveat 3. To date, there's been extensive media coverage of the VA matter but most of it is repetitious and does not provide specific input to veterans regarding many actions they can take to protect themselves. I have benefited by several web sites whose names and internet addresses are provided in this report. I strongly recommend they be thoroughly reviewed as they are all quite informative and some are very detailed.

PERSONAL PROACTIVE ACTIONS

I. CREDIT BUREAUS:

1. Call each of three credit bureaus at their toll free numbers; advise your personal information was stolen (tell them you are one of the affected veterans or others affected by the VA mishandling of your personal information. When you call, do the following:

- A. As a victim of this, or any future financial crime, you are entitled to a free copy of your credit bureau record. Ask for a copy of your file to be sent to you.
- B. Ask to have a 90 day fraud alert immediately put on your file.

1) Supposedly, any financial organization you now do business with will be alerted of the fraud alert when they next review your file. They might contact you personally to verify anything pertinent to your record with them because of the alert. **HOWEVER,**

2) NOTE: This writer has had fraud alerts on all three credit bureau records for over two years. No business has ever contacted me about anything although many have reviewed my records.

3) Additionally, I was victimized in 2005 when unknown person(s) contacted a bank and changed my home address and phone number pertaining

to my credit card. This bank never contacted me although 7-year fraud alerts were on my credit bureau records. As a result, the bank complied with the criminals instructions by changing my personal information, and for several months, my credit card account was used without my knowledge. I never received statements during this period because they were mailed to the wrong (false) address in two different states. It wasn't until I tried using the card that I learned the account was closed because of unpaid bills. It took this writer five months to resolve this problem, but had the bank originally checked with me when the change of address was submitted, they would have immediately learned that criminals were attempting to steal my identity and use my account. Naturally, the identities of the culprits were never known to the bank and no law enforcement agency expressed an interest in this case. Losses amounted to approximately \$1800.

- 4) The lack of statements was not an indicator me that something was amiss. Financial institutions do not necessarily send a statement if an account is not used. Since I wasn't using the credit card I wasn't surprised when monthly statements didn't arrive. Only because I attempted to use the card did I learn problems existed and my account was closed.

- C. You can also write a letter to each credit bureau providing them your SSN and requesting they put a 7-year extended fraud alert on your credit bureau file. You must also provide them a copy of a document such as your driver's license, bank statement or utility statement to confirm your address.
- D. The extended alerts will be documented in your file so the next time you receive a copy of your credit bureau report, you'll see the fraud alert annotated in the report.
- E. In your letter to the credit bureaus, you can also OPT-OUT of the credit bureau promotional programs. That means if you specifically request this, *your file will be annotated and the credit bureaus will not provide your personal information to companies seeking to sell you products or services. Having a "promotional block" is one way to reduce the number of businesses possessing your personal information.*
- F. The Fair Credit Reporting Act entitles every consumer to one free report per year and this doesn't count the free report you receive because you are a victim.
- You should wait three to five months after you receive your initial credit bureau report and then contact each of the credit bureaus again and ask for your annual free copy. Once you receive it, compare it against the first one to identify any discrepancies.
 - Every time you receive your credit bureau reports, review them in depth for accuracy. Mistakes should be documented. At the back of the reports, you'll find forms to complete and return, identifying

those listings or information you challenge.

- Insure you retain copies of all communications with the credit bureaus or notes of any telephone conversations you may have with one of their representatives.
- It is not necessary to contact the credit bureaus frequently as information won't change that often. Once you get a report, take action where needed on erroneous entries but don't needlessly communicate with the credit bureaus or repeatedly ask for reports which won't change but occasionally.

2. CREDIT (security) FREEZE

A. The Consumer Union defines a credit, or security freeze as "a right of the consumer to freeze access to the credit file held by a consumer reporting agency about that consumer. The consumer can give access to selected users of the credit file through a password or a temporary exemption to the freeze." A freeze can be effective in blocking unauthorized changes in your financial history or erroneous information from being placed in your credit bureau records. On the other hand, if you attempt to obtain "instant credit" at anytime, that too could be affected because your credit history will be delayed to a new company until you "lift" the freeze for them.

A. Irrespective of the pros and cons, it's sad to say that a majority of American consumers and veterans do

not have the right to "freeze" their credit bureau records. Only some states have passed laws allowing consumers in their states to take this action while other states for whatever reason, haven't yet acknowledged the rights of their citizens.

B. Unfortunately, businesses, direct marketers and others seeking to sell you the sun, do not want you to be able to protect yourself from their unwanted solicitations, thus, they lobby politicians to not pass such legislation. Following are states with credit freeze laws. If your state is not listed below, it's incumbent upon you to contact your state legislator and tell him or her you want credit freezes to be authorized in your state. States that now have such laws are as follows:¹⁷

- 1) California
- 2) Colorado
- 3) Connecticut
- 4) *Texas - ONLY ID THEFT VICTIMS*
- 5) Louisiana
- 6) Vermont
- 7) *Washington-ONLY ID THEFT VICTIMS*
- 8) Nevada
- 9) Illinois
- 10) Maine
- 11) New Jersey
- 12) North Carolina
- 13) Florida
- 14) Kentucky
- 15) Minnesota

¹⁷. <http://www.bankrate.com/brm/news/cc/20030613c2.asp> Identity stolen? "Freeze your credit report" By Amy C. Fleitas and Dani Arthur & <http://www.consumersunion.org/campaigns/financialprivacynow/learn.html>

- 16) New Hampshire
- 17) New Jersey
- 18) New York
- 19) Oklahoma
- 20) Utah
- 21) Wisconsin
- 22) *Hawaii - ONLY ID THEFT VICTIMS*
- 23) *Kansas - ONLY ID THEFT VICTIMS*
- 24) *South Dakota-ONLY ID THEFT VICTIMS*

D. On June 20, 2005, the Washington Monthly published an article by Kevin Drum. Following is an extract of that article.

“When a business — or a fake business run by ID thieves — requests a credit report, normal practice is for the report to be immediately turned over with no questions asked. A "credit freeze" is an option that turns this around: if you put a freeze on your account, lenders are prohibited from reviewing your credit report unless you give your permission. This prevents most ID fraud since lenders generally refuse to issue credit without first seeing a credit report.... Consumers should have absolute control over their own credit information. This is especially true given the skyrocketing incidence of ID fraud and the [obvious inability of credit agencies to keep personal information secure](#). It's time to shut down the ID thieves, and this is the way to do it. Someone needs to start making a stink about this in Congress.”

E. A very good explanation about credit freeze's can be found on the web site of the California Department of Consumer Affairs, Office of Privacy Protection. The URL is: <http://www.privacy.ca.gov/sheets/cis10securityfreeze.pdf>

F. The same office provides extensive and valuable information on Identity Theft issues in general and the URL for that information is: <http://www.privacy.ca.gov/cover/identitytheft.htm>

II OPT-OUT OPTIONS - A variety of laws allow consumers to "OPT-OUT" of various direct marketing business processes routinely and commonly employed by businesses nationwide. It is imperative that veterans take advantage of these legal processes and have their identities and personal data removed from direct marketing lists. The more lists we are on, the more opportunity exists that our personal information is captured and retained by businesses and organizations that at some point, will lose our information or in some other way, fail to safeguard from criminals seeking to exploit the information. Following are some recommendations that all veterans consider:

1. Credit Bureaus

A. As stated above (page 15), a consumer can request a "Promotional Block" from the three major credit bureaus. This is requested in writing and when instituted, is supposed to keep the credit bureaus from selling your personal information to direct marketers and direct mailers.

2. Direct Marketing Association - Have you ever wondered how so many organizations and businesses get your name and other personal information. There is an entire industry that exists exclusively for the purpose of acquiring and reselling your personal information. A major player in that industry is the Direct Marketing Association (DMA). It is very important that veterans take appropriate steps to reduce their vulnerabilities by having their personal information protected from as many unnecessary direct marketing lists as possible. Here's how to do it:

- Go to the following URL:

<http://www.dmaconsumers.org/consumerassistance.html>

- The above URL has links to the following:

a. [How to remove your name from mailing lists.](#)

Some consumers would like to receive less advertising mail at home. Mail Preference Service (MPS) is designed to assist those consumers in decreasing the amount of national nonprofit or commercial mail they receive at home. You can register online, or via mail.

Here is an extract from this site:
<http://www.dmaconsumers.org/cgi/offmailinglist>

"To receive less commercial advertising mail, you can register for The DMA's Mail Preference Service (MPS)

Please note, The DMA does not provide marketers with consumer mailing lists or do consumer mailings. Rather, the Mail Preference Service is available to companies for the sole purpose of removing your name and address from their mailing lists. This service does not apply to mail sent to your business address, or to "resident/occupant" mail.

What are the expected results?

When you register with MPS, your name and address are placed on a "do-not-mail" file. All DMA members are required to run their list of prospective customers against the MPS file, to remove the individuals who have registered with MPS from their mailings. The service is also available to non-members of The DMA, so that all marketers may take advantage of this service to eliminate the names of those who wish to receive less unsolicited mail.

This "do not mail" file is updated monthly and distributed four times a year -- January, April, July, and October (some mailers receive the file monthly). Your name remains on file

for five years, after which time you may register again.

Although registration with MPS will help to reduce the amount of unsolicited mail that you receive, it will not stop all unsolicited mail. You may continue to receive mail from companies with which you already do business and from non-DMA organizations which do not use MPS. In addition, you may continue to receive mail from local merchants, professional and alumni associations, political candidates and office holders."

b. [How to get your name off telemarketing lists.](#)

Some consumers would like to receive fewer telephone marketing calls at home. The Telephone Preference Service (TPS), a do-not-call service, is a service to assist those consumers in decreasing the number of national commercial calls received at home. You can register online, or via mail.

Here is an extract from this site:

<http://www.dmaconsumers.org/cgi/offtelephone>

"The DMA does not provide marketers with consumer telephone lists or telemarket to consumers. Rather, the Telephone Preference Service is available to companies for the sole purpose of removing your telephone number from their telemarketing lists. This service does not apply to telemarketing at your business number.

The registration form [below](#) will allow you to significantly reduce the amount of unsolicited telemarketing calls you receive at home. You may register with TPS by filling out this form, then clicking on the submit button. For more details, read "[How to register for TPS](#)" below."

c. [How to get your name off e-mail lists.](#)

Sponsored by the Direct Marketing Association, this service allows consumers to indicate that they wish to reduce the amount of unsolicited commercial e-mail they receive. Consumers register and, for security purposes, re-confirm their individual registration with the e-Mail Preference Service (e-MPS).

Here is an extract from this site:

http://www.dmaconsumers.org/consumers/optoutform_emps.shtml

"Use the registration form below to register with the e-MPS.

- e-MPS is the [E-mail Preference Service](#) and allows you to "opt out" of national e-mail lists. [Find out more about e-MPS](#).

You will continue to receive e-mail from groups or advertisers who do not use e-MPS to clean their lists.

Although registration with e-MPS will help reduce the number of e-mails you receive, it will not stop all commercial e-mails. You may continue to receive e-mails from groups or advertisers who do not use e-MPS to clean their lists. E-mail of a business-to-business nature received at your place of employment is also not affected through registration with e-MPS.

The DMA does not provide marketers with consumer e-mail lists."

d. [How to remove deceased individuals names from marketing lists.](#)

The DMA sometimes receives calls from family members, friends or caretakers seeking to remove the names of deceased individuals from commercial marketing lists. To assist those who are managing this process the DMA has created a new Deceased Do Not Contact List (DDNC).

Here is an extract from this site:

<https://preference.the-dma.org/cgi/ddnc.php>

"To assist those who are managing this process, DMA created (in October 2005) a Deceased Do Not Contact List (DDNC) which all DMA members are required to honor. The Deceased Do Not Contact List is available to companies and nonprofit organizations for the sole purpose of removing names and addresses from their marketing lists.

How to Register

Friends, relatives and caregivers are encouraged to register the information about deceased individuals as soon as possible. We encourage funeral directors, hospitals, doctors' offices and others to provide this Internet link to the bereaved, as well.

Verification Fee

There is a \$1 credit card verification fee for each consumer registered. This charge serves two important purposes: to make sure we have a permanent record of the credit card information of those who did the registering; and to help prevent misuse of, or fraud against, this system."

- *The following statement is posted on the Direct Marketing web site.*

What is The DMA Privacy Promise?

More than 130 million Americans made a purchase by mail or telephone last year, and many more are now choosing to shop online.

The Direct Marketing Association (The DMA) is the largest trade association for businesses interested in interactive and database marketing. Companies displaying The DMA Member logo have

committed to the association's Privacy Promise which includes the following principles:

- Provide customers with notice of their ability to opt out of information rental, sale or exchange with other marketers.
- Honor your request not to share your information with other marketers.
- Honor your request not to receive mail, telephone or other solicitations again.
- Use the DMA's [Mail Preference Service](#) and [Telephone Preference Service](#), and [E-mail Preference Service](#), national name-removal services of consumers who wish not to receive unsolicited offers at home.
 - The DMA telephone number to OPT-OUT is 212-768-7277

3. [Individual Company Privacy Statements](#) -

- We all receive Privacy Procedures from financial institutions we are associated with. We get them when we open new bank accounts; when we receive new credit cards or open investment accounts or if we initiate any other financial transaction. We receive them whenever changes are made to our accounts, such as changes in interest rates or the day of the month payments are due.
- These Privacy Procedures are generally printed and distributed in small, fold out brochures we receive with account statements.
- At the back of these brochures, consumers are provided a short form to mail to the company or a toll free telephone number to call and "OPT-OUT" of undesired and unsolicited direct mailings from the

company and *third party affiliates!* Sometimes email addresses are provided to OPT-OUT. There is also generally a short statement that your privacy rights may be governed by the state you reside in since different states often have different privacy laws.

- Your rights to OPT-OUT may allow you to stop specific company mailings or more importantly, *third party mailings.*
- It's your choice if you wish to stop receiving unsolicited mailings, but to substantially reduce your vulnerability to identity theft, I recommend OPTING-OUT of anything you can.
- "Opting-out" reduces the number of businesses who possess your personal information. The fewer that possess your information, the safer you are.

4. Other

- Pre-Approved Firm Offers of Credit & Insurance: [1-888-5OPTOUT](tel:1-888-5OPTOUT)
 - A. This is an automated number for the credit bureaus. Although you may have already put a promotional block on your credit bureau records, it doesn't hurt to register with this number to try and reduce the unsolicited, pre-approved credit card applications and insurance offers you receive.
 - B. When you call this number, *do it from your home telephone.* You will be asked to confirm your name, Social Security Number and Date of Birth.

C. The recording will advise you will be opted-out for five years.

D. This is good only for personal solicitations, not for mail sent to businesses.

- No matter what we do, we still receive some offers for insurance, health care and other services and commodities, irrespective of the lists we OPT-OUT of. I OPT-OUT of everything, yet the junk mail continues to arrive, often associated with interests in my life or products related to things I've purchased. Unfortunately, we can't absolutely stop everyone whom we do business with from selling our personal information, but we can sure try to reduce the profiling of our personal lives. A few other miscellaneous suggestions might be worth considering.

A. When you receive solicitation letters from insurance or health companies or agencies soliciting funds, respond with a letter directing your name & personal information be removed from their files and electronic storage media. Advise you have fraud alerts on your credit files, you've opted-out through the Direct Marketing Association (DMA), and you do not want their product. Advise if you continue receiving their unsolicited advertisements, you'll file a complaint with the Federal Trade Commission (FTC), or take stronger action, if warranted.

1) Insure you do all of this in writing.

2) If you respond by mail, your only evidence of their receipt is to pay for signature delivery service. First class mail at this rate costs \$5.40 per letter which can become expensive depending upon the numbers of letters you respond to.

3. An alternative to mail is faxing. Typically, you can call the toll free number on the advertisement, explain you wish to forward written documentation to the company and request a fax number. You'll usually get it, and by faxing your response, you'll have a receipt that your letter arrived at its' destination. As most of us have our own fax equipment, the cost is substantially less than postage stamps or signature services.

4. Maintain all documentation in case you need it again, in the future.

B. Any unsolicited mail containing any of your personal information must be shredded. Never throw anything away unless it's destroyed sufficiently so that your information cannot be recovered by dumpster divers!

Additional Related Information

1. There are many valuable resources currently available for anyone believing they are a victim of Identity Theft or other financial crimes.

A. National Criminal Justice Reference Service
www.ncjrs.org/spotlight/identity_theft/programs.html

▪ This section provides examples of State and local programs and initiatives available online.

- [Arizona](#)
- [California](#)
- [Colorado](#)
- [Delaware](#)
- [Florida](#)
- [Georgia](#)
- [Indiana](#)
- [Kentucky](#)
- [Massachusetts](#)
- [Michigan](#)
- [Minnesota](#)
- [Mississippi](#)
- [Nebraska](#)
- [North Carolina](#)
- [North Dakota](#)
- [Ohio](#)
- [Texas](#)
- [Utah](#)
- [Virginia](#)
- [Washington](#)
- [National](#)

This site provides specific details associated with the above listed states & services.

B. Jones Library - Identity Theft

<http://www.joneslibrary.org/ref/identitytheft.html>

"Please keep in mind when viewing these Identity Theft Tips that the tips are to be used for information and reference only. The Federal and State laws are changing rapidly to stem the tide of rising Identity Theft. Check with the Federal Trade Commission and/or your state's attorney general's office or a legal professional for help concerning existing laws, as well as concerns about future changes in the law. Also contact any financial institution such as banks and credit card companies as to their policies and procedures if you have any questions. Policies and time periods may vary from those listed in the following information."
[excellent resource]

- Removing your name from pre-approved credit card and insurance offer lists will not keep you from getting mortgage refinancing and home equity loan offers. You will need to call the Acxiom U.S. Consumer Hotline at 877-774-2094 or send a request to Dataquick, Attn: Opt-Out Dept., 9620, Towne Center Drive, San Diego, CA 92121. [According to this web site, if you have already OPTED-OUT of the DMA lists, you do not have to contact this agency.]

C. "Contact the major check verification companies (listed in the [CalPIRG-Privacy Rights Clearinghouse checklist](#)) if you have had checks stolen or bank accounts set up by an identity thief. In particular, if you know that a particular merchant has received a check stolen from you, contact the verification company that the merchant uses:"¹⁸

- CheckRite -- (800) 766-2748
- ChexSystems -- (800) 428-9623 (closed checking accounts)
- CrossCheck -- (800) 552-1900
- Equifax -- (800) 437-5120
- National Processing Co. (NPC) -- (800) 526-5380
- SCAN -- (800) 262-7771
- TeleCheck -- (800) 710-9898

¹⁸. <http://www.usdoj.gov/criminal/fraud/idtheft.html>

D. Some additional web sites pertaining to Identity Theft.¹⁹

▪ *Government - United States:*

[California Department of Consumer Affairs
Consumer.gov](#)
[Federal Bureau of Investigation](#)
[Federal Deposit Insurance Corporation](#)
[Federal Trade Commission - Congressional Testimony](#)
[Federal Trade Commission - Consumer Alert](#)
[United States Postal Inspection Service](#)
[United States Secret Service](#)

▪ *Non-Government - United States*

[Better Business Bureau - Alert](#)
[Better Business Bureau -- Eastern Massachusetts/Maine/Vermont](#)
[CalPIRG](#)
[Center for Democracy and Technology](#)
[National Association of Attorneys General](#)
[National Consumers League](#)
[National Fraud Information Center](#)
[Privacy Rights Clearinghouse](#)

E. **Privacy Rights Clearing House, Fact Sheet #17, Coping with Identity Theft: Reducing the Risk of Fraud**²⁰ This is a very informative document on how you can reduce your risks to Identity Theft.

F. **Consumer Union - www.FinancialPrivacyNow.org**
An extremely helpful and informative site that provides extensive current information and status on legislative and legal issues around the nation.

G. **2006 Consumer Action Handbook** - An excellent and extensive resource, available at no charge at the following internet address:
www.ConsumerAction.gov

19. *ibid*

20. <http://www.privacyrights.org/fs/fs17-it.htm>

2. Identity Theft "Passport Programs"

A. Not universal in United States.

B. According to an email²¹ I received from Ms. Corrine Vaughan, Virginia Attorney General's Office and Director, Victim Notification Program, the following states in America have "Passport programs."

1. Arkansas
2. Iowa
3. Mississippi
4. Montana
5. Nevada
6. Ohio
7. Oklahoma
8. Rhode Island
9. Virginia

C. States without "Passport" programs for ID Theft victims provide their residents with internet links and other references on how to protect themselves.

D. ID Theft victims who obtain "passports" have an official document that identifies them as an ID Theft victim. When produced for law enforcement or other authorities, this document might assist in protecting an innocent victim from being accused or even arrested of an offense committed by another person in the victim's name.

E. States that do not have "Passport" Programs should consider creating them to help their citizens protect themselves from criminals.

²¹. June 22, 2006 email, 1 pg from Ms. Corrine Vaughan, VA Attorney General Office, subj: ID Theft Passport Programs - Other States

F. On July 7, 2006, Mr. Steve Bucci wrote in an article entitled " Credit monitoring and ID Theft passports,"²²

"I have also recommended that the VA create a Federal Identity Theft Passport that identifies a person as a victim of data theft. There is more than bogus credit accounts at stake here. Veterans could be held accountable for unreported or untaxed earnings by the IRS, crimes committed using false documentation and so on from thieves using their stolen information.

A federal "passport" will help bolster a claim of innocence of any crimes related to a veteran's social security number or possible use of a false identity by a criminal. This document will provide an easily recognizable record that could be used to support assertions of innocence with law enforcement officers, employers, the IRS, creditors, credit bureaus and others. Several states (Nevada, Iowa, Virginia, Oklahoma, Montana, Ohio) currently have ID-theft-passport laws on the books. A federal version is called for, as this problem spans residents of all states and territories."

G. Personally, I strongly endorse the idea of a federal ID Theft Passport, especially since so many people associated with the federal government have become victims of the U.S. Government's inability to adequately protect personal and private information. Even since the VA debacle, other federal agencies, including the US Navy, have either lost personal data or have found it on the internet.

²². July 7, 2006, article entitled "Credit Monitoring and `ID Theft passports," <http://www.bankrate.com/brm/news/debt/20060707a1.asp>

H. Americans can no longer expect their government to adequately protect their personal information. It is incumbent of each of us to take proactive steps to protect ourselves, or to seek our legislators support in voting for meaningful electronic security legislation. We've witnessed too many instances of the failure of political appointees to adequately understand and implement effective IT security measures.

ABOUT THE AUTHOR

I am a retired U.S. Air Force officer with over 20 years of military service in the fields of law enforcement, personnel and information security, criminal investigations and counterintelligence. I was a civilian police officer before joining the Air Force and following my military service, I served as a contractor supporting US Government agencies in varied, analytic duties.

Since 2001, I've been a multiple identity theft victim in addition to having my personal information mishandled, not only by the Veterans Administration but also by a major hospital, several accounting companies two large, national banks and one business that I know of. I've had my personal information incorrectly and intentionally posted on a web site; medical providers routinely mis-billed insurance companies because of their failure to verify my current, correct personal information with hospital admissions personnel. These providers, using contract accounting companies, acquired archived, personal information and erroneously submitted claims to incorrect insurance companies. In the course of writing this document, a USG employee erroneously faxed an official document regarding me, to an unknown recipient. It contained extensive, personal data, including my SSN.

My troubles began in 2001 when a bank customer service representative of a large, national bank, responding to a telephonic inquiry by someone impersonating me, intentionally failed to ask for a password on my password protected accounts, because "bank policies don't require that passwords be verified during telephonic transactions."

I'd urge everyone to ask their bank officials about policies involving telephonic transactions. I am now planning on terminating a 40+ year banking relationship because of repetitive, incompetent handling of my personal information and the indifference expressed to me in response to letters I've written to corporate bank leaders.

A more recent incident involved a different bank changing my personal data to include adding the changed information to my credit bureau records although 7-year fraud alerts existed for two years prior to the bank's actions. This incident took me approximately five months to resolve.

It's unknown why the bank changed my personal data without checking with me first. More importantly, why the credit bureaus accepted the changes in my records is beyond me. Obviously, they don't pay attention when illogical changes are made to records, even when the records are flagged with fraud alerts. That may occur because several of the credit bureaus "outsource" the data input of our financial records to offshore, non-US companies.

The routine neglect of security compliance measures and gross misconduct by both civilian businesses and government personnel have significantly and adversely affected me during the past five years. As a result, I've attempted to reduce my use of credit cards and move towards more cash transactions. Whenever possible, I OPT-OUT of any marketing programs associated with any business, agency or organization I'm affiliated with. I maintain an audit trail on all communications associated with these actions and will not hesitate to take strong measures if others repeatedly ignore my efforts to protect my identity.

These measures will include filing complaints with the Federal Trade Commission and with the Better Business Bureau (BBB) in the city where the violator is domiciled.

Interestingly, none of my encrypted internet banking transactions, purchases through EBay or Amazon.com purchases, have resulted in a single incident. Conversely, all the incidents that affected me were caused by sloppy, complacent and lazy behavior of so called "trusted" persons, especially bank personnel who I'd opine, were the were offenders.

This document was compiled in an effort to assist others in protecting their personal identities and reputations.

Most of the substantive data in this document is available at the referenced internet web sites and many other locations at both state and federal levels. The listed, large non-profit organizations involved in assisting Americans and residents in combating identity theft provide very important and valuable information, and should be coordinated with by anyone suspecting they are an identity theft victim.

In states where laws pertaining to credit freezes and ID Theft Passports are lacking, residents should insist of their state and national legislators, that corrective measures be taken and adequate laws be passed.

If we as citizens say and do nothing, the interests of corporations; direct mailers, direct marketers, the credit bureaus and those who make a profit off the sale of our personal information will endure. We will continue to be bombarded by invasive and unsolicited "promises" for credit cards we won't use and we don't need; for insurance we don't want and for other financial commitments that do not serve us well. Our information will be constantly at risk and we will suffer.

So what will you do - wait while others fight this battle on your behalf?

Our only option is to be smarter and take the appropriate steps to reduce the threat.

Ed Lawton
USAF retired
elawton@cox.net