National Archives and Records Administration

8601 Adelphi Road
College Park, Maryland 20740-6001

Fact Sheet
Regarding the National Archives and Records Administration
Breach of a Hard Drive Containing Personally Identifiable Information (PII)

1. What happened?

The National Archives and Records Administration (NARA) learned in late March 2009 that an external hard drive containing a copy of Clinton Administration Executive Office of the President data is missing from a NARA processing room in our College Park, MD facility. The hard dive includes files that contain personally identifying information (PII). The drive was being used for routine recopying to ensure preservation of the information. Approximately 113 4mm tape cartridges were copied onto a two terabyte Western Digital MY BOOK external hard drive.

2. What types of personally identifying information (PII) was stored on the hard drive?

Because some of the EOP offices engaged in personnel related work (e.g., the Office of Administration and the Presidential Personnel Office) or maintained electronic files containing privacy information, such as White House entry information, the external drive contains PII, including names and social security numbers for former Clinton Administration staff and persons who contacted or visited the White House complex.

3. I worked in the Executive Office of the President during the Clinton Administration; how can I tell if my information was compromised?

At this point, there is no evidence that any missing data has been used improperly. However, the National Archives and Records Administration is asking everyone affected by this breach to be vigilant and to carefully monitor any suspicious activity related to your identity. You do not have to close your bank accounts or cancel your credit cards; however you should take steps to protect yourself. Please read the points below on how to protect yourself from identity theft and what you should do if you suspect that you are a victim of identity theft.

4. What is identity theft?

Identity theft occurs when your personal information is stolen and used to commit fraud or other crimes.

5. How can I protect myself against suspicious or unusual activity?

We advise the following steps:

- Review your credit reports. By law you are entitled to one free credit report each year from each major credit bureau. Request a free credit report from one of the three major credit bureaus – Equifax, Experian, and TransUnion – at http://www.annualcreditreport.com/ or by calling 877-322-8228.

- Watch for other suspicious activity related to your identity (see section 6 below).

- Consider enrolling in the free credit monitoring that NARA is offering, through Experian's Triple Alert program. Triple Alert will alert you when changes are posted to your credit report. Details on enrolling in Triple Alert are in the enclosed letter.

  If you have already used your free annual credit report this year, credit reports are also available at a highly discounted rate through your Triple Alert membership.

  Triple Alert will inform you about new items that post to your credit reports from the time you enroll, but you must also go through all the information currently in your credit reports and review them for suspicious activity. Be sure to review all alerts from Triple Alert for suspicious activity.

  You must enroll in Triple Alert to get the benefits of credit monitoring, identity theft insurance and fraud resolution services.

- Additionally, you may wish to review the Federal Trade Commission booklet, "Taking Charge: Fighting Back against Identity Theft," to help you remedy the effects of an identity theft. It describes what steps to take, your legal rights, how to handle specific problems you may encounter on the way to clearing your name, and what to watch for in the future. The booklet is available at www.ftc.gov/bcp/edu/pubs/consumer/idtheft/idt04.shtm.

- For additional information on how to guard against misuse of personal information, visit the Federal Trade Commission website at www.ftc.gov.

6. What kind of suspicious activity should I watch out for?

Suspicious activities could include the following:

- Credit inquiries from companies you haven't contacted or done business with;
- Purchases or charges on your accounts you didn't make;
- New accounts you didn't open or changes to existing accounts you didn't authorize;
- Bills that don't arrive as expected;
- Unexpected credit cards or account statements;
- Denials of credit for no apparent reason; and,
- Calls or letters about purchases you didn't make.

7. Can I receive free credit monitoring?

Yes. The National Archives and Records Administration is offering Triple Alert, a free credit monitoring service from Experian, for individuals affected by this breach. Registration is completely complimentary and enrolling in this program will not affect your credit score. Registration for free credit monitoring service is open for two months from the date of the accompanying letter.

To activate your complimentary one year membership in Triple Alert, visit the website listed below and enter your individual activation code from the notification letter that was enclosed. If you prefer, you can enroll on the phone by speaking with Experian's Customer Care specialists toll-free at **888-451-6553**.

Experian Web Site: http://partner.consumerinfo.com/nara

The credit monitoring services include automatic daily monitoring alerts documenting any changes to your credit report and monthly "no hit" alerts if no changes are detected in a given month. Triple Alert includes customer care and fraud resolution services to assist you in resolving any problems that may arise on your credit report. Triple Alert also includes $25,000 in identity theft insurance coverage with no deductible to cover certain expenses related to identity theft (note that ID Theft Insurance is not available in New York).

8. What should I do if I have a suspected or actual case of identity theft?

If you have an actual or suspected case of fraud, if you see something suspicious on your credit reports or one of your accounts, or if there is something on your credit reports that you do not understand, contact Experian's Triple Alert Customer Care immediately at 888-451-6553. Your issue will be handled by an Experian Fraud Resolution Agent who will help you understand the item in question and walk you through the resolution process, which may include some or all of the following steps:

- Reviewing your credit reports
- Disputing inaccurate or fraudulent items
- Closing fraudulent or compromised accounts
- Filing a police report
- Filing a complaint with the FTC
- Filing a complaint with your state Attorney General (see http://www.naag.org/ to determine your AG)
- Filing a Fraud Alert

- Filing an Identity Theft Insurance Claim

Experian's Fraud Resolution Team will review your individual situation and walk you through the steps necessary to resolve the issue. All of the above items, including information on filing insurance claims and setting fraud alerts, are available online on the Triple Alert web site after you enroll in Triple Alert. If you have any questions about these items or the resolution process, contact Triple Alert Customer Care at **888-451-6553**.

You must enroll in Triple Alert to get access to the Triple Alert Fraud Resolution Service.

9. How long has the hard drive been missing?

The missing hard drive was last seen sometime between October 2008 and the first week of February and was discovered missing on or about March 24, 2009.

10. What are the records on the hard drive?

The 4mm tapes that were copied onto the hard drive generally comprised "snapshots" of the contents of hard drives of departing EOP employees, and therefore contain a mix of system and working files. The drive contains copies of both federal and Presidential records, depending on which EOP office the files came from.

11. Are the Clinton Administration records that were stored on the hard drive permanently lost?

No original records have been lost. NARA has the original tapes and a backup of the hard drive.

12. How did NARA learn that the hard drive was missing?

Work on examining the hard drive was halted because the processing office wanted to investigate using automated tools to generate inspection reports. This would have reduced the amount of time that staff needed to spend validating the data on the hard drive. Staff discovered the hard drive was missing when the hard drive analysis project restarted.

13. What is the National Archives doing about the situation?

- NARA's Office of Inspector General, with the assistance of the United States Secret Service, has launched a full-scale criminal investigation into this incident. NARA is offering a reward of up to $50,000 for information leading to the recovery of the missing hard drive (see more detailed information in paragraph 20, below).

- NARA informed the U.S. Computer Emergency Readiness Team of the Department of Homeland Security, the White House Counsel's Office, staff of our House and Senate Oversight Committees, and the representative of former President Clinton.

- NARA is sending notification letters to affected individuals and offering free credit monitoring services to help protect individuals from identity theft. These letters are being sent on a rolling basis, as we identify particular individuals.

- NARA is revising its internal policies and procedures to ensure maximum protection of electronic and textual records containing PII. NARA is also implementing stringent physical and technical safeguards in place to protect personal information and prevent this type of incident from occurring in the future. Other initiatives include annual and refresher training for our employees and contractors to ensure they are familiar with privacy rules, regulations and standard operating procedures aimed at reducing the risk of breaches of PII.

14. What is the earliest date at which suspicious activity may have occurred due to this data breach?

The loss of the external hard drive was first discovered on March 24, 2009. However, the drive was last accounted for sometime between October 2008 and early February 2009. Thus, if the data has been misused or otherwise

used to commit fraud or identity theft crimes, it is possible that affected individuals could have suspicious activity beginning as early as October 2008.

16. Can Social Security put a flag on my number?

No, unlike the credit bureaus, the Social Security Administration (SSA) cannot put a flag or security alert of any type on your Social Security number. To report that someone is using your Social Security number,, see section 7 above titled, "What should I do if I have a suspected or actual case of fraud or identity theft."

17. Can I get a new Social Security number?

If you have done all you can to fix the problems resulting from misuse of your Social Security number and someone still is using your number, the Social Security Administration may assign you a new number.

Note, however, you cannot get a new Social Security number:

- To avoid the consequences of filing for bankruptcy;
- If you intend to avoid the law or your legal responsibility; or
- If your Social Security card is lost or stolen, but there is no evidence that someone is using your number.

If you decide to apply for a new number, you will need to prove your age, U.S. citizenship or lawful immigration status, and identity. You also will need to provide evidence that you are being disadvantaged by the misuse of your social security number. For additional information, you may wish to contact the Social Security Administration by phone at 800-772-1213 or via their website at http://www.ssa.gov/.

18. Where can I get more information?

If your questions are not answered in this Fact Sheet, you may wish to contact the NARA Breach Response call line at **877-281-0771** or **301-837-3769**, or contact us by e-mail at breach_response@nara.gov. Someone from NARA will respond to your inquiry.

19. Who should I contact if I have any information about the missing hard drive?

NARA is offering a reward of up to $50,000 for information leading to the recovery of the missing Western Digital MY BOOK external hard drive containing personally identifiable information (PII). Anyone who can provide information leading to the recovery of the external hard drive should call the USSS Washington Field Office at **202-406-8800**. This Hot Line is manned and operated by representatives of the United States Secret Service. A cash reward of up to $50,000 will be paid for information provided that leads to the recovery of the MY Book external hard drive.