

Rick Stephens  
Senior Vice President  
Human Resources and  
Administration

The Boeing Company  
100 N Riverside MC 5003-6028  
Chicago, IL 60606-1596



I am writing to let you know that a Boeing laptop was stolen from an employee's car in early December. The laptop is believed to contain unencrypted files with personally identifiable employee data. Those files contain the names and Social Security numbers of approximately 382,000 past and present Boeing employees and in most cases home address, home phone number, date of birth and/or salary. Your information is included in one of the files. No banking, credit card or password information was on file in the stolen laptop.

Know that there is no evidence at this time that any information contained on this or any previously stolen Boeing computer has been accessed, used or disclosed.

However, because of the personal nature of the data we are taking every precaution which includes acting as if data has been compromised.

To protect individuals affected by this personal data loss, Boeing is partnering with ConsumerInfo.com, an Experian® company in offering 3-years of Triple Advantage<sup>SM</sup> credit monitoring protection.

To protect your credit, you should activate your Triple Advantage<sup>SM</sup> membership as soon as you possibly can. You must sign up yourself by April 15, 2007. Neither Boeing, nor anyone else, can do it for you.

To complete the activation process, you need to use a special assigned promotional code.

Your Promotional code is XXXXXXXXXX

To immediately activate your credit monitoring membership, go to the Experian website: <http://partner.experiantdirect.com/premium/default.aspx?sc=655900>.

For answers to Frequently Asked Questions and step-by-step instructions for enrolling in the credit monitoring membership online go to the Boeing Personal Data Loss Web site at <http://www.boeing.com/empinfo/dataprivacy/>.

Your credit monitoring product, Triple Advantage<sup>SM</sup>, will identify and notify you of any key changes that may be a sign of Identity Theft. Your membership includes:

- One 3-Bureau Report when you sign up
- Unlimited access to your Experian Credit Report and Credit Score

- Daily monitoring of all three of your national Credit Reports
- Email or SMS Text alerts when key changes are identified
- \$50,000 Identity Theft insurance provided by Virginia Surety Company, Inc.\*
- Access to dedicated Fraud Resolution representatives

\*Due to New York state law restrictions, coverage cannot be offered to residents of New York.

If you have questions about this credit monitoring product, call ConsumerInfo.com at 1-866-617-1920. ConsumerInfo.com's hours are Monday through Friday 6 a.m. to 6 p.m. and Saturday-Sunday 8 a.m. to 5 p.m. Pacific Time.

For the latest information on this personal data loss go to:

- Boeing's external site at <http://www.boeing.com/empinfo/dataprivacy/>
- Boeing's internal site at <http://boeingit.web.boeing.com/index.aspx?com=3&id=1>

Because personally-identifiable information is required in many Human Resources processes, we have implemented a three-phase plan aimed at better protecting employee information.

1. We have taken steps to replace individual's Social Security Numbers with other identifiers wherever possible and significant progress has been made.
2. We also required the removal of personally-identifiable information from the hard drives of Boeing computers; required confirmation that the removal had been completed; ensured software to encrypt data was installed on computers for those few occasions when data needs to be downloaded; and trained all employees who deal with personally-identifiable information to ensure the policy, requirements and processes were understood. This incident resulted from violation of our requirements.
3. The third phase of the plan is automatic encryption of all information on Boeing computers. This phase began this month and is a requirement for all Boeing computers beginning with those of employees who work with personally-identifiable information and other Boeing proprietary information.

The news of this personal data loss is truly a regrettable event. Having been the victim of identity theft in the past, I well understand the concerns of affected individuals. On behalf of Boeing, I apologize for the inconvenience and frustration this causes you.

Sincerely,



Senior Vice President  
Human Resources and Administration

---

---

---

---

## **Personal Data Loss – December 2006 Frequently Asked Questions**

### **1 - What happened?**

A Boeing laptop computer was stolen from an employee's car the first week of Dec. The laptop is believed to contain unencrypted files that contained personally identifiable employee data. Those files contain the names and social security numbers of approximately 382,000 past and present Boeing employees and in most cases home address, home phone number, date of birth and/or salary. The employee is authorized to use the information for work and believed the files were fully deleted. Employees, past and present, not personally notified by Boeing are not affected.

### **2 - If the employee deleted the files and believes he or she emptied the recycle bin, why is this then considered a personal data loss?**

It is important to note here that even if the files were deleted and the recycle bin was emptied, that action merely removes the "file placement marker." The file will not show up in the directory, but the file contents are still present on the hard drive until overwritten by a new file. A computer savvy individual could retrieve deleted file contents. To protect our employees, Boeing therefore considers the files to be "unsecured" and open to compromise by unauthorized persons. The data is split across numerous separate files.

### **3 - What is "Personally Identifiable Information"?**

Personally Identifiable Information, or PII, is the combination of any information that can be used to identify a person such as:

- First name OR first initial and last name in combination with one or more of the following: Social Security number, Driver's license number, State ID number, Home address.
- Financial account numbers, credit or debit card numbers, in combination with any required security code, access code, or password that would permit access to an individual's financial account.

### **4 - What kind of Personally Identifiable Information (PII) is on the files in this stolen laptop?**

First of all, no banking or credit card information was these files. But names, addresses, home phone numbers and Social Security numbers were in the files for all affected individuals.

### **5 - Why was my personal information on a laptop computer?**

The files in question involved Human Resources-related activities and working with them is part of the employee's statement of work.

### **6 - Who is affected?**

This incident affects 382,000 individuals, most of them former employees/retirees. Each individual, active and inactive, is being personally notified by the company. Employees, current and past, not personally notified by Boeing, are not affected.

### **7 - What is Boeing doing to lessen the potential for identity theft in this situation?**

Boeing is personally contacting each affected person and offering them a 3-year credit monitoring membership at no charge. Within 90 days, affected individuals must activate their credit monitoring membership themselves.

### **8 – What can I do to protect my credit?**

Follow the direction the notification letter and activate your credit monitoring membership as soon as you possibly can. Affected individuals must activate their credit monitoring membership them self by April 15, 2007.

**9 – I don't have easy access to a computer how do I activate my credit monitoring membership.**

If you don't have easy access to a computer, you can call ConsumerInfo.com at 1-866-617-1920. ConsumerInfo.com's hours are Monday through Friday 6 a.m. to 6 p.m. and Saturday-Sunday 8 a.m. to 5 p.m. Pacific Time. Remember to save the notification letter you received from Boeing, you will need to follow the information in it to fill out the credit monitoring membership papers.

**10 - I received a similar notice during the past year about a personal data loss and signed up for credit monitoring then. Do I need to do anything now?**

Continue to monitor your credit report. You do not need to re-enroll; your membership has automatically been extended for another year for a total of four years from your original activation date.

**11 - What is Boeing doing to prevent future loss of personal data via computer thefts?**

Because personally-identifiable information is required in many company processes, we have implemented a three-phase plan aimed at better protecting employee information.

1. We have taken significant steps to replace individuals' Social Security Numbers with other identifiers wherever possible and much progress has been made.
2. We also required the removal of personally-identifiable information from the hard drives of Boeing computers and required confirmation that the removal had been completed. We've ensured software to encrypt data was installed on computers for those few occasions when data needs to be downloaded, and trained all employees who deal with personally-identifiable information to ensure the policy, requirements and processes were understood. This incident resulted from violation of our requirements.
3. The third phase of the plan is automatic encryption of all information on Boeing computers. This phase began this month and is a requirement for all Boeing computers beginning with those of employees who work with personally-identifiable information and other Boeing proprietary information.

**12 - If Boeing made it mandatory for personal information files to be encrypted, why wasn't this file encrypted?**

The employee was only using the files temporarily and he/she thought deleting the files from his/her laptop was a sufficient way to dispose of the files.

**13 - What has happened to the employee?**

As this is a personnel matter, Boeing can make no comment regarding the employee. Upon completion of the investigation, appropriate corrective action will be taken as warranted.

**14 - What is happening with the investigation?**

Boeing is working with authorities in an effort to recover the laptop.

**15 - Haven't there been similar incidents of stolen laptops with unencrypted personal information?**

Yes, there have been several incidents of laptops being stolen from Boeing employees. That's why the above mentioned efforts are being taken to safeguard our employees and their personal information.

**16 - Has there been any identity theft linked to this or previous incidents?**

There is no evidence at this time that identity theft has taken place as a result of either this or any previous Personal Data Losses at Boeing.