



Legal Department
55 Glenlake Parkway, NE
Atlanta, GA 30328

June 8, 2007

Ms. Kelly A. Ayotte
Attorney General
State of New Hampshire
33 Capitol Street
Concord, NH 03301

RE: Report of breach of security involving personal information

Dear Attorney General Ayotte:

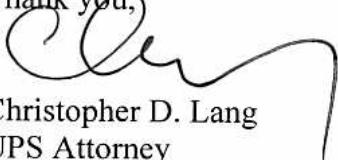
We are writing to inform you, pursuant to requirements of RSA 359-C:20(I)(b), that we will soon be mailing notification to 142 employees of UPS in New Hampshire that sensitive information related to them was accessed by a then-UPS employee who was not authorized to obtain the information.

During a routine information systems audit in February of this year, we discovered that names, Social Security Numbers, employee identification numbers, and job classification and status information had been downloaded to a UPS computer from our network by an employee of UPS. The information appears to have been downloaded along with an unrelated software program that we believe was the focus of the download. We immediately initiated a comprehensive forensic investigation of the incident, and we did not find any evidence that the employee intended to access, misuse or disclose the information. However, because we are not able to determine conclusively that the information was not subject to misuse or additional disclosure, we have notified affected individuals of the incident in an abundance of caution so they may take steps to protect against fraud or misuse of the information.

We expect to send the notifications to the 142 affected individuals in New Hampshire by June 11, 2007. A copy of the letter we will be sending is attached for your files.

We are available to answer any questions you may have about this incident. Please contact me at 404-828-7174 if you have any questions and if we can provide additional information.

Thank you,


Christopher D. Lang
UPS Attorney

[UPS LETTERHEAD]

[Date]

[Employee Name]

[Address]

[City], [State] [Zip]

Re: Notice Regarding Potential Unauthorized Access To Employment-Related Information

Dear [Name],

We are writing to advise you that we have discovered that a former employee of UPS, while still employed by UPS, may have accessed certain information relating to your employment on UPS computer systems. During a recent audit of UPS information systems we discovered that information about you and certain other present and former UPS employees, consisting of names, Social Security Numbers, UPS Employee Identification Numbers, and job classification and status information, had been downloaded from a database to a computer workstation at a UPS facility. The information appears to have been downloaded along with an unrelated software program that we believe was the focus of the download.

The information that this former employee downloaded does not appear to have been subject to misuse or disclosed to anyone else. But we are notifying you of this incident in an abundance of caution to provide you with an opportunity to take steps to monitor your financial accounts and to take other precautions to protect yourself against the possibility of financial fraud based upon access to your Social Security Number.

We suggest that you immediately consider taking the steps outlined on the reverse side of this letter, "IMPORTANT STEPS TO HELP PREVENT FRAUD." This sheet includes explanations as to how these actions can help protect you from becoming a potential victim of identity theft.

We regret any inconvenience to you and we stand ready and willing to provide assistance. Please call on us at 1-800-XXX-XXXX if you have any questions.

IMPORTANT STEPS TO HELP PREVENT FRAUD

1. **Carefully review all of your banking and credit card account statements issued since June, 2005, and report any unauthorized transactions.** Although the information involved did not include banking or credit card information, you should review your accounts to make certain there was no unauthorized or suspicious activity on those accounts.
2. **Notify your financial institution(s) and credit card companies that you received this notice.** This will provide them with notice that information relating to you may have been viewed or accessed by an unauthorized party.
3. **Contact the fraud department at the three major credit bureaus listed below and ask them to place a “fraud alert” on your credit file.** When you place an initial fraud alert with one of the bureaus, your request will automatically forward to the other bureaus which will also place fraud alerts on your credit file. *Please note* that placing a fraud alert will make it more difficult for a criminal to open a fraudulent account in your name, but it may also make it more difficult for you to open a new account as well, because extra steps will be required to verify your identity in connection with credit approval processes. You may wish to discuss with the credit bureau when you call how you might minimize inconveniences to you during the time the fraud alert is active.

Experian: (888) 397-3742 or www.experian.com

Equifax: (877) 478-7625 or www.equifax.com

TransUnion: (800) 680-7289 or www.transunion.com

4. **Obtain a copy of your credit report from each of the three major credit bureaus and review them to be sure they are accurate and include only authorized accounts.** You are entitled to one free copy of your report annually. To order your report, you may visit www.annualcreditreport.com or call toll-free (877) 322-8228. Carefully review your credit report to verify that your name, address, account, and any other information is accurate and notify the credit bureaus of any errors you detect.
5. **Visit the Federal Trade Commission’s (“FTC”) website at www.ftc.gov to obtain additional information about how to protect against identity theft.** You may also wish to contact the FTC at (877) FTC-HELP (877-382-4357) or TTY: (866) 653-4261 if you have further general questions about identity theft.
6. **Remain vigilant over the next 12 to 24 months for potential incidents of identity theft or other misuse of personal information.**