

5

**North Carolina Security Breach Reporting Form
Pursuant to the Identity Theft Protection Act of 2005**

Name of Business Owning or Licensing Information Affected by the Breach: United Parcel Service ("UPS")
Address: 55 Glenlake Parkway
Atlanta, GA 30328
Telephone: 404-828-7174
Fax: 404-696-6912
Email: clang@ups.com

PLEASE SUBMIT FORM TO:
Consumer Protection Division
NC Attorney General's Office
9001 Mail Service Center
Raleigh, NC 27699-9001
Telephone: (919) 716-6000
Toll Free in NC: (877) 566-7226
FAX: (919) 716-6050

Date Security Breach Reporting Form submitted: June 21, 2007

Date the Security Breach was discovered: February 22, 2007

Estimated number of affected individuals: 21,902

Estimated number of NC residents affected: 871

Name of business maintaining or possessing information that was the subject of the Security Breach, if the business that experienced the Security Breach is not the same entity as the business reporting the Security Breach (pursuant to N.C.G.S. § 75-65(b)): N/A

Describe the circumstances surrounding the Security Breach and state whether the information breached was in electronic or paper format: During a routine information system audit in February, 2007, we discovered that names, Social Security Numbers, employee identification numbers, and job classification and status information about certain current and former employees of UPS had been downloaded to a UPS computer from our network by a then-UPS employee. 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 internal forensic investigation, which did not uncover any evidence that the employee intended to access the sensitive information. However, because we are unable to determine conclusively that the information was not subject to misuse or further disclosure, we are providing notification to affected individuals so they may take steps to protect against potential fraud.

Regarding electronic information breached, state whether the information breached or potentially breached was password protected or encrypted in some manner. Not encrypted If so, please describe the security measures protecting the information: The only individuals with access to the data were those with "Admin" rights to the system; no other employees had access to the data.

Describe any measures taken to prevent a similar Security Breach from occurring in the future: UPS has removed the Social Security Numbers from the database and now uses employee ID numbers, additionally archived files are no longer kept on the system as they were previously.

Date affected NC residents were/will be notified: June 11, 2007

If there has been any delay in notifying affected NC residents, describe the circumstances surrounding the delay pursuant to N.C.G.S. § 75-65(a) and (c): Necessary time was taken to perform a comprehensive forensic investigation to determine the scope of the breach, which involved interviewing the individual who accessed the information, and to assess the extent to which the data may have been misused.

If the delay was pursuant to a request from law enforcement pursuant to N.C.G.S. § 75-65(c), please include the

written request or the contemporaneous memorandum.

How NC residents were/will be notified?
(pursuant to N.C.G.S. § 75-65(e))

Please attach copy of the notice if in written form or a copy of any scripted notice if in telephonic form.

- written notice
- electronic notice (email)
- telephone notice
- substitute notice

Signature: _____

Date: June 21, 2007

Contact Person, Title: Christopher D. Lang, Attorney

Address: _____

(if different from above) _____

Telephone: 404-828-7174

Fax: 404-828-6912

Email: clang@ups.com

[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 1-866-617-8722 if you have any questions.

Sincerely,

Gary Kallenbach
Administrative Manager

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.**