COLUMBIA UNIVERSITY
IN THE CITY OF NEW YORK
OFFICE OF THE GENERAL COUNSEL

Direct Line: (212) 342-4083
Facsimile: (212) 854-6621

April 23, 2012

By First Class Mail

Attorney General Michael Delaney
New Hampshire Office of the Attorney General
33 Capitol Street
Concord, NH 03301

To whom it may concern:

On April 16, 2012, Columbia University learned for the first time that a file containing personal information of approximately 3,500 current and former employees and sole proprietor contractors had been inadvertently placed on a web server that could be accessed by individuals outside of the University. The University immediately disabled access to the file and promptly commenced an investigation into the matter.

The file was an internal test file created in January 2010 and related to direct deposit reimbursement of expenses or payment for services. It contained the names, addresses, bank account numbers, and Social Security numbers of the affected individuals. However, the file did not contain the names of or other identifying information (e.g., bank routing numbers) of specific financial institutions.

Our audit logs confirm that this file was not accessed from January 2010 until March 10, 2012; on that date, the file was indexed by Google, which meant that the information contained in the file could show up through a Google search. Immediately upon learning that this information was accessible via the Internet on April 16, 2012, the University removed the file from the server and worked with Google to remove the information from Google search results, including cached search results. The University verified that this information had been completely removed – both from the accessible server and from the Google cached search results – on April 17, 2012. We have also verified that this information is not currently available elsewhere on the Internet – such as through other search engines.

Columbia has concluded that this security incident was unintentional, and we do not have evidence of wrongdoing or identity theft.

The relevant files contained the personal information of four New Hampshire residents. We are offering two years of credit monitoring to these individuals. The form of the notice sent to these individuals on April 21, 2012 is attached for your information.

Columbia University deeply regrets that this incident occurred. We are keenly aware of how important it is to safeguard information entrusted to the University. In response, we have taken steps to ensure the situation is not repeated.

If you have any questions about this incident, please do not hesitate to contact me.

Sincerely,

Danna Drori

Danna Drori
Associate General Counsel

Enclosures

April 21, 2012

<<First Name>> <<Last Name>>
<<Address_Line_1>>
<<Address_Line_2>>
<<Address_Line_3>>
<<City>>, <<State>> <<Postal_Code>>

Dear <<First Name>> <<Last Name>>:

On April 16, 2012, Columbia University was first informed that a file containing personal information of approximately 3,000 current and former employees, and 500 sole proprietors, had been inadvertently placed on a web server that could be accessed by individuals outside of the University. The University responded immediately and disabled access to the file.

The file was an internal test file created in January 2010 related to direct deposit reimbursement of expenses. I regret to inform you that the file contained your name, address, Social Security Number, and bank account number used in 2010 for direct deposit reimbursement of expenses. However, the file did not contain the name or other identifying information (e.g., bank routing numbers) of your associated financial institution.

Our audit logs confirm that this file was not accessed from January 2010 until March 10, 2012. On that date, the file was indexed by Google, meaning the information contained in the file could have been available after March 10, 2012 through a Google search. Immediately upon learning that the information in this file was accessible via the Internet, the University removed the file from the server and worked with Google to remove the information from Google search results, including cached search results. The University verified that this information was completely removed – both from the accessible server and from the Google cached search results – on April 17, 2012. We also verified that this information is not currently available elsewhere on the Internet, such as through other search engines.

Columbia has concluded that this security incident was unintentional. We have no evidence of wrongdoing or identity theft. However, we are making this notification consistent with applicable state laws, and in accordance with our privacy policies and procedures.

To safeguard against the possibility of misuse of personal information, Columbia has arranged for you to receive a two-year subscription to the ProtectMyID™ Alert service from Experian, a credit monitoring system, at no cost to you. This service will provide you with a free copy of your Experian credit report, monitor your credit files at all three major credit bureaus (Equifax, Experian and Trans Union), notify you of certain suspicious activities that could indicate identity theft, and provide assistance in the event of any suspected identity theft. As a further precaution, if you are still using the same bank account that you used for direct deposit of expenses in 2010, you may wish to close that bank account and designate a different account for direct deposit expense reimbursements from the University.

Important: If you wish to enroll in the Experian service, you may do so by calling Experian toll-free at 877-371-7902 or visiting their website, www.protectmyid.com/redeem, and entering the following unique, personal redemption code:

<<unique_code>>

To take advantage of this coverage, you must enroll by July 31, 2012.

Even if you do not wish to enroll in the Experian service, there are other steps you can take to help protect yourself, as noted in the attachment titled "Information about Identity Theft Prevention."

Information security is a serious issue for the University, as we know it is for you. Columbia continues to strengthen its measures to protect sensitive information, including the implementation of additional tools to search for sensitive information inadvertently placed in locations that are not secure. We are also strengthening our policies and procedures on where sensitive information should be stored on our systems.

We sincerely apologize for this incident. We take the protection of your identity seriously. If you have any questions or comments, please contact us by calling, toll-free, (877) 634-9701. Additional information is also available at http://cuit.columbia.edu/FAQ-4-21-2012.

Sincerely,

Jeffrey F. Scott
Executive Vice President
Columbia University Student & Administrative Services

Enclosure

Information About Identity Theft Prevention

Regular Review of Account Statements and Credit Reports: You may consider regularly reviewing statements from your accounts and periodically obtaining your credit report from one or more of the national credit reporting companies. You may obtain a free copy of your credit report once every 12 months by visiting http://www.annualcreditreport.com, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to:

Annual Credit Report Request Service
P.O. Box 105281
Atlanta, GA 30348-5281

You can print a copy of the request form at: http://www.ftc.gov/bcp/menus/consumer/credit/rights.shtm. You can also purchase a copy of your credit report by contacting one of the three national consumer reporting agencies:

Equifax
800-525-6285
www.equifax.com
P.O. Box 740241
Atlanta, GA 30374-0241

Experian
888-397-3742
www.experian.com
P.O. Box 9532
Allen, TX 75013

TransUnion
800-680-7289
www.transunion.com
Fraud Victim Assistance Division
P.O. Box 6790
Fullerton, CA 92834-6790

Once you receive your credit reports, we urge you to review them carefully for inquiries from companies you did not contact, accounts you did not open, and debts on your accounts that you cannot explain. Verify the accuracy of your complete name, Social Security Number, address(es), and employer(s). Notify the three consumer reporting agencies listed above if any information is incorrect.

We recommend you remain vigilant with respect to reviewing your account statements and credit reports over the next 12 to 24 months and promptly report any suspicious activity or suspected identity theft to proper law enforcement authorities, including local law enforcement, your state's attorney general and the Federal Trade Commission (FTC). You may contact the FTC to obtain additional information about avoiding identity theft.

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20580
1-877-IDTHEFT (438-4338)
http://www.ftc.gov/idtheft

You may obtain information from the FTC and the consumer reporting agencies listed above about fraud alerts and security freezes. We also provide some additional information about fraud alerts and security freezes below.

Fraud Alerts: There are two types of fraud alerts that you can place on your credit report to put your creditors on notice that you may be a victim of fraud: an initial alert and an extended alert. An initial fraud alert stays on your credit report for at least 90 days. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An extended fraud alert stays on your credit report for seven years. You can have an extended alert placed on your credit report if you have been a victim of identity theft and you provide the credit reporting company with

the documentary proof it requires. You can place a fraud alert on your credit report by calling the toll-free fraud number of any of the three credit reporting companies provided above.

Security Freeze: You may request a "security freeze" on your credit file. The security freeze will prohibit a consumer reporting agency from releasing any information in your credit file without your express authorization. A security freeze is designed to prevent credit, loans or services from being approved in your name without your consent. You should be aware that using a security freeze may delay, interfere with, or prevent the timely approval of any subsequent request or application you make regarding new loans, credit, mortgage, insurance, government services or payments, rental housing, employment, investment, license, cellular phone, utilities, digital signature, internet credit card transactions, or other services. In addition, you may incur fees to place, lift, and/or remove a credit freeze, which generally range from $5-$20 per action. Since the instructions for how to establish a credit freeze differ from state to state, please contact the three major credit reporting companies at the numbers above to find out more information.