MARSHALL, DENNEHEY, WARNER, COLEMAN & GOGGIN
A PROFESSIONAL CORPORATION www.marshalldennehey.com

1845 Walnut Street · Philadelphia, PA 19103-4797
(215) 575-2600 · Fax (215) 575-0856

PENNSYLVANIA
Bethlehem
Doylestown
Erie
Harrisburg
King of Prussia
Philadelphia
Pittsburgh
Scranton
Williamsport

NEW JERSEY
Cherry Hill
Roseland

DELAWARE
Wilmington

OHIO
Akron

FLORIDA
Ft. Lauderdale
Jacksonville
Orlando
Tampa

NEW YORK
New York

January 7, 2011

VIA OVERNIGHT MAIL
Office of the Attorney General
33 Capitol Street
Concord, NH 03301
Attention: Attorney General Delaney

Re: Tulane University Incident Notification

Dear Attorney General Delaney:

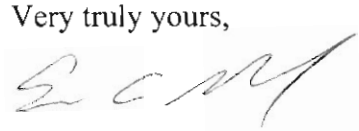
On December 29, 2010, a Tulane University laptop with a file on it containing university employees' W-2 information, including names, social security numbers, addresses and salary information was stolen. This incident affects individuals employed by Tulane in 2010 and individuals who will receive a Tulane University issued 2010 W-2, including student employees and part-time employees. It does not affect the entire Tulane student body. The password-protected laptop was not encrypted and was located in a briefcase that was stolen from the locked automobile of a university employee who was traveling outside New Orleans. The employee had the laptop and information in order to prepare W-2 forms over the university winter holiday. Generally, university employees do not store this information on laptops. The incident was immediately reported to the appropriate police department and they are conducting an investigation. To date, the laptop has not been recovered.

We have no reason to believe that this was a targeted theft seeking the information contained on the laptop. Furthermore, we have not received any evidence that the data involved in this incident has been improperly accessed or misused. As a precautionary measure, we are notifying all affected individuals of this incident and offering them one year of credit monitoring through TransUnion. Additionally, we have set up a call center to answer the questions of affected individuals and to assist those individuals with enrolling in credit monitoring. There are 23 New Hampshire residents potentially affected by this incident. Notification is being sent to those affected residents in the form attached hereto.

Tulane University has in place administrative and technical procedures consistent with safeguarding personal information. As soon as the university learned of the theft, it started a review of its policies and procedures concerning the use and protection of confidential information. Additionally, the university is re-educating its employees with respect to safeguarding laptops and confidential information. Tulane University

will continue to take the necessary and appropriate steps to further secure all personal information in order to help avoid any future incidents.

Very truly yours,



Eric A. Packel

EAP/mp

Enclosure

01/6514166.v1

Return mail will be processed by: IBC
P.O. Box 802
Fort Mill, SC 29716-0802
PO #5021
19 36 00006154 801255

Tulane University
6823 St. Charles Avenue
New Orleans, LA 70118

January 6, 2011

Dear :

The privacy and confidentiality of the personal information of our students and employees is a top priority at Tulane University. Regrettably, we are writing to you because of an incident involving some of your personal information.

On December 29, 2010, a university laptop with a file on it containing your W-2 information, including your name, social security number, address and salary information was stolen. The password-protected laptop was not encrypted and was located in a briefcase that was stolen from the locked automobile of a university employee who was traveling outside New Orleans. The employee had the laptop and information in order to prepare W-2 forms over the university winter holiday. Generally, our employees do not store this information on laptops. The incident, which affects only those employed by Tulane University in 2010 or those who will receive a Tulane University issued 2010 W-2, was reported to the appropriate police department and they are conducting an investigation.

Law enforcement officials estimate there are over 250 auto burglaries every day in the location where the theft occurred. We have no reason to believe that this was a targeted theft seeking the information contained on the laptop. In fact, personal property of the employee was also stolen from the vehicle. Although we do not have any evidence that the data involved in this incident has been improperly accessed or misused, we wanted to make you aware of the incident and urge you to take the steps described below to safeguard against identity fraud.

Because protecting your personal information is important to us, we have arranged for you to enroll, at no cost, in an online three-bureau credit monitoring service for one year provided by TransUnion Interactive. TransUnion Interactive is a subsidiary of TransUnion, one of the three major nationwide credit reporting companies. To enroll in this service, go to the TransUnion Interactive Web site at **www.transunionmonitoring.com** and in the space referenced as "Activation Code", enter [redacted] and follow the simple steps to receive your services online within minutes.

If you do not have access to the Internet and wish to enroll in a similar offline, paper-based, credit monitoring service, please call [redacted] Monday through Friday, 8:00 a.m. to 6:00 p.m. Central time, 9:00 a.m. to 7:00 p.m. Eastern time. When prompted, please enter or say the following six-digit telephone pass code: [redacted] You can sign up for the online or offline credit monitoring service anytime between now and April 15, 2011. Unfortunately, due to privacy laws, the university cannot register you directly.

Once you are enrolled, you will be able to obtain one year of unlimited access to your TransUnion credit report and credit score. The daily 3-bureau credit monitoring service will notify you if there are any critical changes to your credit files at TransUnion, Experian and Equifax, including fraudulent activity, new inquiries, new accounts, new public records, late payments, change of address and more.

Whether or not you choose to use TransUnion Interactive's credit monitoring services, we recommend that you remain vigilant to the possibility of fraud and identity theft by reviewing your credit card, bank, and other financial statements for unauthorized activity. You may also obtain a copy of your credit report, free of charge annually, directly from each of the three nationwide credit reporting companies. To order your free report visit www.annualcreditreport.com, or call toll free at 1-877-322-8228, or write to the following addresses:

Equifax	Experian	TransUnion
1-800-525-6285	1-888-397-3742	1-800-680-7289
P.O. Box 740241	P.O. Box 9554	P.O. Box 6790
Atlanta, GA 30374	Allen, TX 75013	Fullerton, CA 92834
www.equifax.com	www.experian.com	www.transunion.com

You also have the right to ask that the nationwide credit reporting companies place a Fraud Alert on your credit file to let potential credit grantors know to verify your identification before extending credit in your name in case someone is using your information without your consent. This is a free service and must be renewed every 90 days. A Fraud Alert can make it more difficult for someone to get credit in your name; however, please be aware that it also may delay your ability to obtain credit. You can call one of the three major nationwide credit reporting companies to place your initial 90-day Fraud Alert: TransUnion (1-800-680-7289); Equifax (1-800-525-6285) or Experian (1-888-397-3742). As soon as the credit reporting company confirms your Fraud Alert they will also forward your alert request to the other two nationwide credit reporting companies so you don't need to contact each of them separately.

If you believe you are the victim of identity theft or have reason to believe your information is being misused, you should immediately contact the police in your jurisdiction and file a police report of identity theft. Obtain a copy of the police report as you may need to provide copies of the report to creditors to clear up your records. You should also contact the attorney general's office in your home state.

We also urge you to take advantage of the call center to answer any questions you may have about the incident and its effects on you personally. The call center, available at [redacted], Monday through Friday, 8 a.m. to 6 p.m. Central time, pass code [redacted] will also help you with enrolling in credit monitoring if you have any questions about that process.

We deeply regret that this event occurred. As soon as we learned of the theft, we started a review of our policies and procedures concerning the use and protection of confidential information. Additionally, we are re-educating our employees with respect to the safeguarding of confidential information. We will make every effort to prevent this type of event from happening in the future.

Sincerely,

Anne P. Baños
Vice President for Administrative Services

Charlie McMahon
Vice President for Information Technology
Chief Technology Officer

00005164
801255