LEWIS BRISBOIS BISGAARD & SMITH LLP
ATTORNEYS AT LAW

550 E. Swedesford Road, Suite 270
Wayne, Pennsylvania 19087
Telephone: 215.977.4100
Fax: 215.977.4101
www.lewisbrisbois.com

JENNIFER A. COUGHLIN
DIRECT DIAL: 215.977.4081
JENNIFER.COUGHLIN@LEWISBRISBOIS.COM

April 22, 2016

VIA U.S. MAIL

Attorney General Joseph Foster
Office of the New Hampshire Attorney General
Attn: Security Breach Notification
33 Capitol Street
Concord, NH 03301

Re: **Notice of Data Security Incident**

Dear Attorney General Foster:

We represent the University of the Southwest ("USW"), 6610 N. Lovington Highway, Hobbs, New Mexico 88242, and are writing to notify you of a data security incident that may affect the security of personal information of one (1) New Hampshire resident. This notice will be supplemented if any new significant facts arise subsequent to its submission. By providing this notice, USW does not waive any rights or defenses regarding the applicability of New Hampshire law or personal jurisdiction.

Nature of the Data Security Event

On or around February 2, 2016, USW discovered that the W-2's of some current employees may have been subject to unauthorized access and used to file fraudulent tax returns. These W-2s are stored on a portal maintained by USW's third-party vendor that hosts employee W-2s and other payroll and tax-related documents. In immediate response to the incident, USW changed all credentials necessary to access employee information on the Greenshades portal and launched an investigation, retaining third-party forensic investigators to assist. The investigation determined that the W-2s and other employee wage or tax-related information stored on the Greenshades portal relating to certain additional current and former employees may have been accessed by an unknown third party; however, actual unauthorized access and/or acquisition of this information has not been confirmed.

Notice to New Hampshire Residents

On April 21, 2016, written notice was provided to the one (1) New Hampshire resident whose information was stored on the Greenshades portal and potentially subject to unauthorized access, in substantially the same form as the letter attached hereto as ***Exhibit A***.

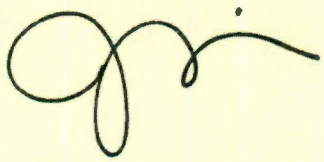
Other Steps Taken and To Be Taken

In addition to taking steps to further secure the information and providing written notice of this incident to all affected individuals as described above, USW is providing affected individuals with access to twelve (12) months of free credit monitoring and identity restoration services, as well as helpful information on how to protect against identity theft and fraud. USW is also providing written notice of this incident to other state regulators where required.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at 215-977-4081.

Very truly yours,



Jennifer A. Coughlin of
LEWIS BRISBOIS BISGAARD & SMITH LLP

Encl.

EXHIBIT A

University of the Southwest

Notice of Data Breach

April 21, 2016

«First_Name» «Last_Name»
«Street_Address_1_»
«Street_Address_2»
«City_», «State_» «Zip»

Dear «First_Name»:

The University of the Southwest ("USW") is writing to inform you of a recent incident that may affect the security of your personal information. We are providing this notice to ensure that you are aware of the incident, so that you may take steps to protect your personal information should you feel it is appropriate to do so.

What Happened. USW uses a third-party vendor to host its employee W-2 and wage information. On February 2, 2016, USW learned that unauthorized access to certain current and former employee W-2s stored on the third-party vendor's portal may have occurred.

What Information Was Involved. USW immediately launched an investigation into the incident. The investigation is ongoing. While there is no indication your W-2 or any other information was subject to unauthorized access, we believe there is a possibility yourW-2 from calendar year 2015 or earlier, which contains your name, Social Security number, contact information, and salary information, or potentially other wage or tax-related information hosted by the third-party vendor may have been accessed without authorization.

What We Are Doing. USW takes the security of your information very seriously. Upon learning of the unauthorized access, we launched an investigation to determine the breadth of the incident. We also changed and strengthened the credentials necessary to access the third-party vendor's portal, and restricted access to it. We are also providing notice of this incident to you, along with information on how to better protect against identity theft and fraud, and access to credit monitoring services with LifeLock. You will be able to enroll to receive these services until June 30, 2016 and, once enrolled, will receive these services until July 1, 2017. The enclosed Privacy Safeguards contains information on protecting against identity theft and fraud and instructions on how to enroll and receive the complimentary credit monitoring services.

What You Can Do. You can review the additional information included in the attached Privacy Safeguards Information on how to better protect against identity theft and fraud. You can also enroll to receive the complimentary access to credit monitoring and identity restoration services with LifeLock.

For More Information. Should you have any questions regarding this incident, please call Ron McBee, Monday through Friday, 8:00 a.m. to 5:00 p.m. M.D.T. at (575) 492-2116.

We sincerely apologize for the inconvenience and concern this event has caused you. We want to assure you that we continue to take appropriate actions to protect the privacy and security of your information.

Sincerely,

Ronald McBee
Vice President and Chief Financial Officer

University of the Southwest
6610 Lovington Highway, Suite 510 | Hobbs, NM 88240
(575)492-2116 | f (575) 392-6006 | www.usw.edu

PRIVACY SAFEGUARDS

To help detect the possible misuse of your information, we are offering enrollment with LifeLock's Benefit Elite credit monitoring and identity restoration services at no cost to you. Please see the attached information for enrollment instructions. You are eligible to enroll to receive these services until June 30, 2016. Once enrolled, you will receive these services until July 1, 2017.

You may take action directly to further protect against possible identity theft or financial loss. We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports and explanation of benefits forms for suspicious activity. Under U.S. law you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report.

At no charge, you can also have these credit bureaus place a "fraud alert" on your file that alerts creditors to take additional steps to verify your identity prior to granting credit in your name. Note, however, that because it tells creditors to follow certain procedures to protect you, it may also delay your ability to obtain credit while the agency verifies your identity. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts on your file. Should you wish to place a fraud alert, or should you have any questions regarding your credit report, please contact any one of the agencies listed below.

Equifax	Experian	TransUnion
P.O. Box 105069	P.O. Box 2002	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19022-2000
800-525-6285	888-397-3742	800-680-7289
www.equifax.com	www.experian.com	www.transunion.com

You may also place a security freeze on your credit reports. A security freeze prohibits a credit bureau from releasing any information from a consumer's credit report without the consumer's written authorization. However, please be advised that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing, or other services. If you have been a victim of identity theft, and you provide the credit bureau with a valid police report, it cannot charge you to place, list or remove a security freeze. In all other cases, a credit bureau may charge you a fee to place, temporarily lift, or permanently remove a security freeze. You will need to place a security freeze separately with each of the three major credit bureaus listed above if you wish to place a freeze on all of your credit files.

To find out more on how to place a security freeze, you can use the following contact information:

Equifax Security Freeze	Experian Security Freeze	TransUnion
P.O. Box 105788	P.O. Box 9554	PO Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19022-2000
1-800-685-1111	1-888-397-3742	www.transunion.com/securityfreeze
(NY residents please call 1-800-349-9960)	www.experian.com/freeze/center.html	1-888-909-8872
www.equifax.com/help/credit-freeze/en_cp		

You can further educate yourself regarding identity theft, and the steps you can take to protect yourself, by contacting your state Attorney General or the Federal Trade Commission. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue, NW, Washington, DC 20580, www.ftc.gov/idtheft, 1-877-ID-THEFT (1-877-438-4338); TTY: 1-866-653-4261. Instances of known or suspected identity theft should be reported to law enforcement, your Attorney General, and the FTC. You can also further educate yourself about placing a fraud alert or security freeze on your credit file by contacting the FTC or your state's Attorney General. For North Carolina residents, the Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, (919) 716-6400, www.ncdoj.gov.