MARSHALL DENNEHEY
WARNER COLEMAN & GOGGIN
ATTORNEYS-AT-LAW WWW.MARSHALLDENNEHEY.COM
A PROFESSIONAL CORPORATION
2000 Market Street, Suite 2300 · Philadelphia, PA 19103
(215) 575-2600 · Fax (215) 575-0856

PENNSYLVANIA
Allentown
Doylestown
Erie
Harrisburg
King of Prussia
Philadelphia
Pittsburgh
Scranton
NEW JERSEY
Cherry Hill
Roseland
DELAWARE
Wilmington
OHIO
Cincinnati
Cleveland
FLORIDA
Ft. Lauderdale
Jacksonville
Orlando
Tampa
NEW YORK
Long Island
New York City
Westchester

Direct Dial: 215-575-2615
Email: djshannon@mdwcg.com

February 22, 2018

Via Email: attorneygeneral@doj.nh.gov
Attorney General Joseph Foster
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

RE: University of Wisconsin-Superior Alumni Association
Our File No. 21263.00244

Dear Attorney General Foster:

Pursuant to N.H. Rev. Stat. Ann. § 359-C:20(I)(b), we are writing to notify you of a data security incident involving 3 New Hampshire residents. We are submitting this notification on behalf of our client, the University of Wisconsin-Superior Alumni Association.

Nature Of The Security Breach

On February 1, 2018, UW-Superior Alumni Association sent its alumni a Mississippi River Cruise brochure sponsored by the UW-Superior Alumni Association. In the process of preparing the mailing data, an ID number was sent to UW-Superior Alumni Association's travel vendor and appeared above each individual's name and address on the brochure. On February 5, 2018, UW-Superior Alumni Association was made aware that the ID number for its alumni who graduated during a certain time period may have been the same as the student ID number (social security number) used while in attendance at UW-Superior. As a result, some of the personal information belonging to New Hampshire residents who are UW-Superior alumni may have been exposed to others, including their first and last names, home addresses, and social security numbers.

The residents involved in this incident were forwarded letters notifying them of this incident on February 22, 2018. A copy of the form letter is attached hereto.

Steps Taken Relating To The Incident

Upon learning of this situation, UW-Superior Alumni Association advised UW-Superior Foundation, which owns and controls the data. UW-Superior Foundation took steps to address this incident promptly after it was discovered, including undertaking an internal investigation of the matter in order to develop a better

understanding of what had taken place and how. UW-Superior Foundation took immediate action to ensure it does not happen again, including cleaning the alumni and friend database and replacing all of the "old" ID numbers. UW-Superior Alumni Association's travel vendor has also verified the deletion of all mailing data used for this brochure. UW-Superior Foundation is in the process of reviewing its internal policies and data management protocols and has implemented enhanced security measures to help prevent this type of incident from recurring in the future.

UW-Superior Alumni Association has also arranged to have LifeLock protect the affected individuals' identity and credit for one year at no cost to them through its identify theft protection and credit monitoring services.

Should you need additional information regarding this matter, please contact me.

Very truly yours,

David J. Shannon

DAVID J. SHANNON

DJS:jl
Encl.

UW-Superior Alumni Association
PO Box 2000
Superior, WI 54880

<<Mail ID>>
<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>>
<<Address 5>>
<<City>><<State>><<Zip>>
<<Country>>

<<Date>>

NOTICE OF DATA BREACH

Dear alumni and friend,

We are writing to notify you of a data breach at the UW-Superior Alumni Association that may have involved some of your personal information. The privacy and protection of your information are matters that we take very seriously. Please be assured that we have taken every step necessary to address the incident and that we are committed to fully protecting all of the information that you have entrusted to us. Please review the information provided in this notice for some steps that you may take to protect yourself against any potential misuse of your information.

What Happened

On February 1, you were sent a Mississippi River Cruise brochure sponsored by the UW-Superior Alumni Association. In the process of preparing the mailing data, an ID number was sent to our travel vendor and appeared above your name and address on the brochure.

On February 5, 2018, we were made aware that the ID number for our alumni who graduated during a certain time period may have been the same as the student ID number (social security number) used while in attendance at UW-Superior.

While this was not a "system hack" or a "cyber-attack" as the result of malicious actions, we are acting in an abundance of caution in alerting you to this situation. You may or may not have noticed this number on your brochure. There is no law enforcement investigation concerning this incident.

What Information Was Involved

The personal information that may have been viewable on the brochure included first and last names, home addresses and social security numbers.

What We Are Doing

After learning of this situation, our team took immediate action to ensure it doesn't happen again, to include cleaning the alumni and friend database and replacing all of the "old" ID numbers. Go Next, our travel vendor, has also verified the deletion of all mailing data used for this brochure.

We take our responsibility of protecting your personal data seriously. Therefore, we have retained LifeLock to provide you one (1) year of complimentary identify theft protection and credit monitoring services. To "activate" your membership, call 1-800-899-0180 or go online at https://store.lifelock.com/enrollment?promocode=UWSAA2018. You will need to provide a Membership ID. Your Membership ID is your first name last name plus 5-digit zip code. The enrollment period will expire on March 30, 2018.

What You Can Do

You can take the following steps to guard against identity theft and fraud:

- Register for the complimentary identify theft protection and credit monitoring services provided at no cost to you, as discussed in this notice.

- Review the enclosed "Information About Identity Theft Protection" reference guide, which describes additional steps that you may take to help protect yourself, including recommendations by the Federal Trade Commission regarding your identity theft protection.

For More Information

Please accept our apology, and know protecting your personal information is important to us. If you have any questions, please call us at 715-394-8452.

Sincerely,

Peter D. Nordgren
Chair, UW-Superior Alumni Association

Information about Identity Theft Prevention

We recommend that you regularly review statements from your accounts and periodically obtain your credit report from one or more of the national credit reporting companies. You may obtain a free copy of your credit report online at www.annualcreditreport.com, by calling toll-free 1-877-322-8228, or by mailing an Annual Credit Report Request Form (available at www.annualcreditreport.com) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. You may also purchase a copy of your credit report by contacting one or more of the three national credit reporting agencies listed below.

Equifax: P.O. Box 740241, Atlanta, Georgia 30374-0241, 1-800-685-1111, www.equifax.com

Experian: P.O. Box 9532, Allen, TX 75013, 1-888-397-3742, www.experian.com

TransUnion: P.O. Box 1000, Chester, PA 19022, 1-800-888-4213, www.transunion.com

When you receive your credit reports, review them carefully. Look for accounts or creditor inquiries that you did not initiate or do not recognize. Look for information, such as home address and Social Security number, that is not accurate. If you see anything you do not understand, call the credit reporting agency at the telephone number on the report.

We recommend you remain vigilant with respect to reviewing your account statements and credit reports, and promptly report any suspicious activity or suspected identity theft to the proper law enforcement authorities, including local law enforcement, your state's attorney general and/or the Federal Trade Commission ("FTC"). You may contact the FTC or your state's regulatory authority 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), www.ftc.gov/idtheft

For residents of Maryland: You may also obtain information about preventing and avoiding identity theft from the Maryland Office of the Attorney General:

Maryland Office of the Attorney General, Consumer Protection Division
200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023, www.oag.state.md.us

For residents of North Carolina: You may also obtain information about preventing and avoiding identity theft from the North Carolina Attorney General's Office:

North Carolina Attorney General's Office, Consumer Protection Division
9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-5-NO-SCAM, www.ncdoj.gov

You may want to order copies of your credit reports and check for any bills that you do not recognize. If you find anything suspicious, call the credit reporting agency at the phone number on the report. Keep a copy of this notice for your records in case of future problems with your records. If you are a California resident, we suggest that you visit the web site of the California Office of Privacy Protection at www.privacy.ca.gov to find more information about your privacy.

Fraud Alerts: There are also 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. 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 initial fraud alert stays on your credit report for at least 90 days. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for 7 years. You can place a fraud alert on your credit report by calling the toll-free fraud number of any of the three national credit reporting agencies listed below.

Equifax: 1-888-766-0008, www.equifax.com
Experian: 1-888-397-3742, www.experian.com
TransUnion: 1-800-680-7289, fraud.transunion.com

Credit Freezes: You may have the right to put a credit freeze, also known as a security freeze, on your credit file, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate a freeze. A credit freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a credit freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a credit freeze may delay your ability to obtain credit. In addition, you may incur fees to place, lift and/or remove a credit freeze. Credit freeze laws vary from state to state. The cost of placing, temporarily lifting, and removing a credit freeze also varies by state, generally $5 to $20 per action at each credit reporting company. *Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company.* Since the instructions for how to establish a credit freeze differ from state to state, please contact the three major credit reporting companies as specified below to find out more information:

Equifax:	P.O. Box 105788, Atlanta, GA 30348, www.equifax.com
Experian:	P.O. Box 9554, Allen, TX 75013, www.experian.com
TransUnion LLC:	P.O. Box 2000, Chester, PA, 19022-2000, freeze.transunion.com

You can obtain more information about fraud alerts and credit freezes by contacting the FTC or one of the national credit reporting agencies listed above.