LEWIS BRISBOIS BISGAARD & SMITH LLP

Lindsay B. Nickle
2100 Ross Avenue, Suite 2000
Dallas, TX 75201
Lindsay.Nickle@lewisbrisbois.com
Direct: 214.722.7141

January 4, 2023

VIA ONLINE SUBMISSION
Attorney General Aaron Frey
Maine Attorney General's Office
Consumer Protection Division
6 State House Station
Augusta, ME 04333

Re: Notice of Data Security Incident

Dear Attorney General Frey:

Lewis Brisbois represents Knox College, a private liberal arts college in Galesburg, Illinois, in connection with a recent data security incident described in greater detail below. The purpose of this letter is to notify you that the personal information of certain Maine residents may have been involved in a recent data security incident.

1. Nature of the Security Incident

On November 24, 2022, Knox discovered unusual network activity and learned that it was the victim of a ransomware attack. Knox immediately took steps to secure its network and initiated an investigation with the assistance of cybersecurity experts. The investigation revealed that an unknown actor gained access to and obtained data from the Knox network without authorization on or around November 24, 2022. On December 7, 2022, after a comprehensive review of the potentially impacted data, Knox determined that personal information may have been involved. Since that time, Knox has worked diligently to identify current contact information needed to notify all potentially affected individuals.

2. Type of Information and Number of Maine Residents Affected

On January 3, 2023, Knox notified 124 Maine residents whose personal information may have been involved in this matter. A sample copy of the notification letter is attached. The type of information involved varied by individual but may have included the Maine residents' names, addresses, dates of birth, Social Security numbers, driver's license numbers, and passport numbers. Knox is not aware of the misuse of any information that may have been involved in this incident.

3. Steps Taken Relating to the Incident

As soon as Knox discovered this incident, it took steps to secure its systems and launched an investigation to determine what happened and whether personal information had been accessed or acquired without authorization. Knox has also implemented additional security features to help ensure the security of its systems and reduce the risk of a similar incident occurring in the future.

Knox has established a toll-free call center through IDX to answer questions about the incident and address related concerns. In addition, Knox is offering 12 months of complimentary credit and identity theft monitoring services to all potentially affected individuals. In addition, Knox reported this incident to the Federal Bureau of Investigation and will cooperate with investigative requests in an attempt to hold the perpetrator(s) of this incident responsible.

Knox is continuing to collect up-to-date address information needed to notify all potentially affected individuals. This project is ongoing, and Knox will provide you with supplemental notice should notification be provided to additional residents in your state.

4. Contact Information

Knox remains dedicated to protecting the information in its control. If you have any questions or need additional information, please do not hesitate to contact me at (214) 722-7141 or by e-mail at Lindsay.Nickle@lewisbrisbois.com.

Sincerely,

Lindsay B. Nickle of
LEWIS BRISBOIS BISGAARD & SMITH LLP

Encl.: Consumer Notification Letter Template

KNOX COLLEGE
Return Mail to IDX
P.O. Box 989728
West Sacramento, CA 95798-9728

To Enroll, Please Call:
1-833-758-4141
Or Visit:
https://app.idx.us/account-creation/protect
Enrollment Code: <<ENROLLMENT>>

<<NAME>>
<<NAME2>>
<<COMPANY>>
<<ADDRESS1>>
<<ADDRESS2>>
<<CITY>>, <<STATE>> <<ZIP>>
<<COUNTRY>>

January 3, 2023

Re: Notice of Data <<Variable Text 1>>

Dear <<First>> <<Last>>,

We are writing to inform you of a data security incident that may have affected your personal information. Knox College ("Knox") takes the privacy and security of your personal information very seriously. This is why we are informing you of this incident, providing you with steps you can take to help protect your personal information, and offering you complimentary credit monitoring and identity protection services.

What Happened: On November 24, 2022, Knox discovered unusual network activity and learned that it was the victim of a ransomware attack. We immediately took steps to secure our network and initiated an investigation with the assistance of cybersecurity experts. The investigation revealed that an unknown actor gained access to and obtained data from the Knox network without authorization on or around November 24, 2022. On December 7, 2022, after a comprehensive review of the potentially impacted data, Knox determined that personal information may have been involved. Since that time, Knox has worked diligently to identify current contact information needed to notify all potentially affected individuals.

What Information Was Involved: The information affected may have included your name, address, date of birth, Social Security number, driver's license number, and passport number.

What We Are Doing: As soon as Knox discovered the incident, we took the steps referenced above. In addition, we reported the incident to the Federal Bureau of Investigation and will cooperate with any investigation. We also implemented additional security features to reduce the risk of a similar incident occurring in the future and will continue to evaluate ways to further enhance the security of our network as the investigation progresses. Additionally, we are providing you with information about steps you can take to help protect your personal information.

In addition, we are offering you complimentary credit monitoring and identity protection services for <<12/24>> months through IDX, a national leader in identity protection services. The IDX services, which are free to you upon enrollment, include a subscription for the following: single bureau credit monitoring, CyberScan dark web monitoring, fully-managed identity recovery services, and $1 million in identity theft insurance coverage. With this protection, IDX will help you resolve issues if your identity is compromised

What You Can Do: Please review this letter carefully, along with the guidance included with this letter about additional steps you can take to protect your information. In addition, we encourage you to enroll in the credit monitoring and identity theft protection services we are offering through IDX. To receive credit monitoring services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

You can enroll in the free IDX identity protection services by calling 1-833-758-4141 or going to https://app.idx.us/account-creation/protect and using the Enrollment Code provided above. IDX representatives are available Monday through Friday from 8:00 a.m. to 8:00 p.m. Central Time. Please note the deadline to enroll is April 3, 2023.

For More Information: If you have questions or need assistance, please call 1-833-758-4141, Monday through Friday from 8:00 a.m. to 8:00 p.m. Central Time. IDX representatives are fully versed on this incident and can help answer questions you may have regarding the protection of your information.

On behalf of Knox, thank you for your understanding about this incident.

Sincerely,

Bradley Nolden
Vice President for Administration and General Counsel
Knox College

Steps You Can Take to Protect Your Personal Information

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (FTC).

Copy of Credit Report: You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting http://www.annualcreditreport.com/, calling toll-free 1-877-322-8228, 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. You also can contact one of the following three national credit reporting agencies:

Equifax
P.O. Box 105788
Atlanta, GA 30348
1-888-378-4329
www.equifax.com

Experian
P.O. Box 9532
Allen, TX 75013
1-800-831-5614
www.experian.com

TransUnion
P.O. Box 1000
Chester, PA 19016
1-800-916-8800
www.transunion.com

Fraud Alert: You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least one year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at http://www.annualcreditreport.com.

Security Freeze: You have the right to put a security freeze on your credit file for up to one year at no cost. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC, or from your respective state Attorney General about fraud alerts, security freezes, and steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the Attorney General in your state.

Federal Trade Commission
600 Pennsylvania Ave, NW
Washington, DC 20580
consumer.ftc.gov
1-877-438-4338

Maryland Attorney General
St. Paul Plaza
200 St. Paul Place
Baltimore, MD 21202
marylandattorneygeneral.gov
1-888-743-0023

New York Attorney General
Bureau of Internet and Technology Resources
28 Liberty Street
New York, NY 10005
ag.ny.gov
1-212-416-8433 / 1-800-771-7755

North Carolina Attorney General
9001 Mail Service Center
Raleigh, NC 27699
ncdoj.gov
1-877-566-7226

Rhode Island Attorney General
150 South Main Street
Providence, RI 02903
http://www.riag.ri.gov
riag.ri.gov
1-401-274-4400

Washington D.C. Attorney General
400 S 6th Street, NW
Washington, DC 20001
oag.dc.gov
1-202-727-3400

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include to know what is in your file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information; as well as other rights. For more information about the FCRA, and your rights pursuant to the FCRA, please visit https://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf.