



LEWIS BRISBOIS BISGAARD & SMITH LLP

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

August 29, 2022

VIA EMAIL

Attorney General John M. Formella
Office of the Attorney General
Consumer Protection Bureau
33 Capitol Street
Concord, NH 03301
Email: DOJ-CPB@doj.nh.gov

Re: Notification of Data Security Incident

To Whom it May Concern:

We represent Franklin College in connection with a recent data security incident described below. Franklin College is notifying affected individuals and consumer reporting agencies of the incident. The purpose of this letter is to provide formal notice to your office.

I. Nature of Security Incident

On January 21, 2022, Franklin College became aware of unusual activity within its network environment and subsequently discovered that it had been the victim of a data encryption attack by an unknown third party. Franklin College immediately took steps to secure its network environment and launched an investigation. In connection with the investigation, Franklin College engaged a leading digital forensics firm and cybersecurity consultants to determine what happened and whether any sensitive information was affected as a result. The investigation confirmed that personal information had been acquired without authorization. Franklin College engaged an independent data review team to conduct an extensive review of all information which may have been affected. On June 23, 2022, Franklin College determined the scope of the personal information contained within the exfiltrated data. Franklin College then worked diligently to set up the services being offered and locate mailing addresses for potentially affected individuals, which was completed on August 12, 2022.

II. Number of New Hampshire Residents Affected

Based on Franklin College's investigation, a total of two (2) residents of New Hampshire were affected by this incident. The affected information for these individuals includes a name in combination with a Social Security number.

A notification letter was sent to these individuals via first class U.S. mail on August 29, 2022. A sample copy of that notification letter is enclosed.

III. Actions Taken in Response to the Incident

As soon as Franklin College became aware of the potential incident, it launched an investigation, engaged a digital forensics firm to assist with the investigation, and worked to determine whether any personal information was accessed or acquired without authorization. This includes working with leading cybersecurity experts to enhance the security of its network.

Once Franklin College determined which consumers were affected by this incident, it immediately began the process of locating addresses in order to notify them and provide information to consumer reporting agencies regarding the incident. As part of this notice, Franklin College is offering the affected New Hampshire residents twelve (12) months of credit and CyberScan monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed identity theft recovery services. Finally, IDX is staffing a call center available to answer questions and provide support to affected individuals.

IV. Contact Information

If you have any questions or need additional information, please do not hesitate to contact me at 214.722.7141 or lindsay.nickle@lewisbrisbois.com.

Sincerely,

Lindsay B. Nickle of
LEWIS BRISBOIS BISGAARD & SMITH LLP

Encl. Sample Consumer Notification Letter



Return to IDX
P.O. Box 1907
Suwanee, GA 30024

To Enroll, Please Call:
1-833-764-2921
Or Visit:
<https://app.idx.us/account-creation/protect>
Enrollment Code: <<XXXXXXXX>>

<<First Name>> <<Last Name>>
<<Address1>> <<Address2>>
<<City>>, <<State>> <<Zip>>

August 29, 2022

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

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

We are writing to provide you with information about a recent incident that may have involved your personal information. At Franklin College, we take the privacy and security of all of our data seriously. That is why we are sending you this letter telling you about the incident, offering you credit monitoring and identity remediation services, and providing you with information, resources, and steps you can take to help protect your personal information.

What Happened? On January 21, 2022, Franklin College became aware of unusual activity within its network environment. We hired security experts and a computer forensic investigator to help us investigate the incident, ensure the safety of our environment, and determine whether anyone’s personal information was affected. The investigation confirmed that Franklin College was a victim of a malicious code attack. Following this confirmation, we underwent a thorough and extensive review of potentially affected files to determine what personal information may have been involved and identify any potentially impacted individuals. On June 23, 2022, we determined the data viewed or taken by the attacker may have included some of your personal information.

What Information Was Involved? The information that may have been impacted includes your name, <<Variable Data 2>>.

What We Are Doing. We recognize that incidents like this continue to affect large and small companies and organizations throughout the country. We have addressed this matter as thoroughly and expeditiously as possible by conducting a thorough investigation into the incident, implementing additional security measures to enhance the security of our network, and will be continuously evaluating and evolving our current and future cybersecurity practices.

What You Can Do. We have no reason to believe that any of your information has been or will be misused because of this incident. Out of an abundance of caution, we are offering you identity theft protection services through IDX®, the data breach and recovery services expert. These services include: <<12/24>> months of credit and CyberScan monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed identity theft recovery services. We encourage you to review the recommendations on the following page to help protect your information. We also encourage you to contact IDX with any questions and to enroll in the free services we are offering by calling 1-833-764-2921 or going to <https://app.idx.us/account-creation/protect> and using the Enrollment Code provided above. IDX experts are available Monday through Friday from 9:00 am to 9:00 pm ET. Please note the deadline to enroll is November 29, 2022.

For More Information. If you have any questions regarding this incident or would like assistance enrolling in the services offered, please call 1-833-764-2921 Monday through Friday from 9:00 am to 9:00 pm ET. You will need to reference the Enrollment Code at the top of this letter when calling or enrolling online, so please do not discard this letter.

We value your trust in Franklin College, and we regret any inconvenience this unfortunate incident may have caused you.

Sincerely,

Kerry N. Prather
President

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 105851
Atlanta, GA 30348
1-800-525-6285
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 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, and
www.ftc.gov/idtheft
1-877-438-4338

Maryland Attorney General

200 St. Paul Place
Baltimore, MD 21202
oag.state.md.us
1-888-743-0023

New York Attorney General

Bureau of Internet and Technology Resources
28 Liberty Street
New York, NY 10005
1-212-416-8433

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>
1-401-274-4400

Washington D.C. Attorney General

441 4th 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/documents/bcftp_consumer-rights-summary_2018-09.pdf.