

February 24, 2022

VIA ONLINE PORTAL

Attorney General Aaron Frey
Office of the Attorney General
Consumer Protection Division
Security Breach Notification
111 Sewall Street, 6th Floor
Augusta, ME 04330

Re: Notice of Data Security Incident

Dear Attorney General Frey:

Lewis Brisbois Bisgaard & Smith, LLP represents St. Augustine College (“St. Augustine”) in conjunction with a data security incident described in greater details below. St. Augustine is a private college with five locations in Chicago, Illinois. The purpose of this letter is to notify you of the incident in accordance with 10 Me. Rev. Stat. Ann. §§ 1346-1350B.

1. Nature of the Security Incident

On August 7, 2021, St. Augustine detected unusual activity within its digital environment. Upon discovering this activity, St. Augustine immediately engaged a team of cybersecurity experts to secure the environment and conduct an investigation to determine what happened and whether any personal information was accessed or acquired without authorization as a result. The investigation determined that certain files stored on the St. Augustine network may have been accessed or acquired without authorization. St. Augustine then engaged a vendor to review the contents of the impacted systems likely to contain sensitive data. As a result, on February 1, 2022, St. Augustine learned that personal information was involved in the incident. St. Augustine then worked diligently to identify current address information and to notify impacted consumers.

2. Type of Information and Number of Maine Residents Involved

The information involved the name and Social Security number of the impacted residents. St. Augustine notified a single (1) affected Maine resident of this incident via first-class U.S. mail on February 24, 2022. A sample copy of the notification letter is enclosed.

3. Measures Taken to Address the Incident

St. Augustine has taken steps in response to this incident to prevent similar incidents from occurring in the future. In addition, St. Augustine also reported this matter to law enforcement and will provide whatever assistance is necessary to hold the perpetrator(s) responsible. Lastly, St. Augustine is offering the individuals who may have been affected complimentary credit monitoring and identity theft restoration services through IDX, a global leader in risk mitigation and response.

These services include twelve (12) months of credit monitoring and fully managed identity theft recovery services.

4. Contact information.

St. Augustine remains dedicated to protecting personal information in its possession. If you have any questions or need additional information, please do not hesitate to contact me at 214.722.7141 or via email at Lindsay.Nickle@lewisbrisbois.com.

Very truly yours,



Lindsay B. Nickle
LEWIS BRISBOIS BISGAARD & SMITH LLP

Encl: Sample Consumer Notification Letter



Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

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

<<Date>>

Re: Notice of Data Security Incident

Dear <<Name 1>>,

I am writing to inform you of a data security incident experienced by St. Augustine College (“St. Augustine”), that may have involved your personal information. St. Augustine takes the privacy and security of the personal information in our care very seriously. Therefore, we are writing to inform you about the incident and advise you of certain steps you can take to help protect your personal information, and to offer you complimentary credit monitoring and identity protection services.

What Happened? On August 7, 2021, St. Augustine detected unusual activity within its digital environment. Upon discovering this activity, we took immediate and active steps to secure our environment and launched an internal investigation. St. Augustine also engaged cybersecurity experts to secure the environment and conduct an investigation to determine whether any personal information may have been impacted. In the course of investigation, St. Augustine determined that certain files stored on the St. Augustine network may have been accessed or acquired by the unknown actor as a result of this incident. St. Augustine then engaged a vendor to review the contents of the impacted systems likely to contain sensitive data. As a result, on February 1, 2022, St. Augustine learned that your personal information may have been impacted. St. Augustine then worked diligently to identify the current address information required to send notification letters.

What Information Was Involved? The information potentially impacted in connection with this incident may have included your name as well as your <<Breached Elements>>.

What Are We Doing? As soon as St. Augustine discovered the incident, St. Augustine took the steps described above. St. Augustine has also implemented additional safeguards to minimize the chance that an incident like this could occur in the future. Further, St. Augustine reported this matter to the Federal Bureau of Investigation and will provide whatever assistance is necessary to hold the perpetrator(s) of this incident responsible. St. Augustine is also providing you with information regarding steps that you can take to help protect your personal information.

As an added precaution, St. Augustine is offering a one-year membership to TransUnion Interactive’s myTrueIdentity credit monitoring and identity restoration service at no cost to you. This product provides you with premier credit monitoring and identity theft resolution, including up to \$1 million of identity theft insurance coverage.¹ The deadline to enroll in these complimentary services is <<Enrollment Deadline>>.

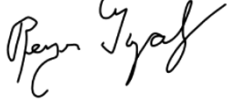
What You Can Do: Although St. Augustine is not aware of any misuse of information as a result of the incident, St. Augustine encourages you to follow the recommendations on the following page to help protect your personal information. In addition, we recommend that you enroll in the complimentary services being offered through TransUnion. Activation instructions and a description of the services are included with this letter.

¹ To receive these services, you must be over the age of 18, 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.

For More Information: If you have questions or need assistance, please contact our team at 855-604-1796, Monday through Friday from 6:00 a.m. to 6:00 p.m. Pacific Time, excluding major US holidays. Call center representatives are fully versed on this incident and can answer any questions that you may have regarding this incident or the complimentary services being offered to you.

Protecting your information is important to us. Please know that we take this incident very seriously, and we regret any worry or inconvenience that this may cause you.

Sincerely,

A handwritten signature in black ink, appearing to read "Reyes González". The signature is fluid and cursive, with the first name "Reyes" and the last name "González" clearly distinguishable.

Reyes González
President
St. Augustine 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 can print this form at www.annualcreditreport.com/cra/requestformfinal.pdf. 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 http://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf.



Activation Code: <<Activation Code>>

Complimentary One-Year *myTrueIdentity* Credit Monitoring Service

As a safeguard, we have arranged for you to enroll, at no cost to you, in an online credit monitoring service (*myTrueIdentity*) for one year provided by TransUnion Interactive, a subsidiary of TransUnion,[®] one of the three nationwide credit reporting companies.

How to Enroll: You can sign up online or via U.S. mail delivery

- To enroll in this service, go to the *myTrueIdentity* website at www.MyTrueIdentity.com and, in the space referenced as “Enter Activation Code,” enter the 12-letter Activation Code <<Activation Code>> and follow the three steps to receive your credit monitoring service 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, via U.S. mail delivery, please call the TransUnion Fraud Response Services toll-free hotline at 1-855-288-5422. When prompted, enter the six-digit telephone passcode <<Engagement Number>> and follow the steps to enroll in the offline credit monitoring service, add an initial fraud alert to your credit file, or to speak to a TransUnion representative if you believe you may be a victim of identity theft.

You can sign up for the online or offline credit monitoring service anytime between now and <<Enrollment Deadline>>. Due to privacy laws, we cannot register you directly. Please note that credit monitoring services might not be available for individuals who do not have a credit file with TransUnion or an address in the United States (or its territories) and a valid Social Security number. Enrolling in this service will not affect your credit score.

ADDITIONAL DETAILS REGARDING YOUR 12-MONTH COMPLIMENTARY CREDIT MONITORING SERVICE:

- 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 credit monitoring service will notify you if there are any critical changes to your credit file at TransUnion, including fraud alerts, new inquiries, new accounts, new public records, late payments, changes of address, and more.
- The service also includes access to an identity restoration program that provides assistance in the event that your identity is compromised and up to \$1,000,000 in identity theft insurance with no deductible. (Policy limitations and exclusions may apply.)