



Lauren D. Godfrey  
One PPG Place, 28<sup>th</sup> Floor  
Pittsburgh, PA 15222  
Lauren.Godfrey@lewisbrisbois.com  
Direct: 412.567.5113

November 4, 2021

**VIA E-Mail**

Attorney General Aaron Frey  
Office of the Attorney General  
Consumer Protection Division  
Security Breach Notification  
111 Sewall Street, 6th Floor  
Augusta, ME 04330  
[breach.security@maine.gov](mailto:breach.security@maine.gov)

Re: Notification of Data Security Incident

Dear Attorney General Frey:

We represent Columbia College of South Carolina in connection with a recent data security incident which impacted one (1) resident of Maine. The incident is described in greater detail below. Columbia College takes the privacy and security of the information within its control very seriously and is taking significant steps to help prevent a similar incident from occurring in the future.

**1. Nature of the data security incident.**

In March 2021, Columbia College detected unusual activity relating to an employee email account. Upon discovering this activity, Columbia College took steps to secure their email system and launched an investigation with the assistance of a leading digital forensics firm to determine what happened and whether personal information may have been accessed or acquired without authorization.

The investigation revealed that one Columbia College employee email account had been accessed without authorization on March 15, 2021. Columbia College then retained a third-party vendor to conduct a comprehensive review of the contents of the account to determine what data might have been involved. Columbia College then worked diligently to identify up-to-date address information to notify impacted individuals which was completed on October 22, 2021.

The impacted data for the impacted Maine Resident includes their name, Date of Birth, Social Security Number, Driver's License Number / State ID Number.

**2. Number of Maine resident(s) affected.**

Columbia College has identified one (1) resident of Maine who may have been impacted by this incident. Columbia College provided notification of the incident to these residents via United States mail on November 4, 2021. A sample copy of the letter is attached.

**3. Steps taken relating to the incident.**

In addition to the steps mentioned above, as soon as Columbia College learned of the incident, it took immediate steps to secure its systems and launched an investigation. Additionally, Columbia College enabled 2 factor authentication throughout their Office 365 environment. Columbia College deployed Sentinel One endpoint detection and response tool throughout the staff network and Office 365 audit logs were enabled. Columbia College limited folder access to individuals with heightened credentials. Columbia College also reported the incident to the United States Federal Bureau of Investigation.

**4. Contact information.**

Columbia College is committed to protecting the sensitive information in its control. If you have any questions or need additional information, please do not hesitate to contact me at (412) 567-5113, or by e-mail at [Lauren.Godfrey@lewisbrisbois.com](mailto:Lauren.Godfrey@lewisbrisbois.com).

Sincerely,

*Lauren D. Godfrey*

Lauren D. Godfrey of  
LEWIS BRISBOIS BISGAARD & SMITH LLP

LDG/sg  
Enclosure



P.O. Box 989728  
West Sacramento, CA 95798-9728

To Enroll, Please Call:  
1-833-513-2602  
Or Visit:  
<https://app.idx.us/account-creation/protect>  
Enrollment Code: <<Enrollment>>

<<FirstName>> <<LastName>>  
<<Address1>>  
<<Address2>>  
<<City>>, <<State>> <<Zip>>

November 4, 2021

**Re:** <<Variable Text 2>>

Dear <<FirstName>> <<LastName>>,

We are writing to inform you of a data security incident experienced by Columbia College, that may have affected your personal information. We are writing to notify you of this incident, to offer you complimentary identity monitoring and protection services, and to inform you about steps that can be taken to help protect your personal information.

**What Happened?** In March, 2021, we detected unusual activity relating to a Columbia College employee email account. Upon discovering this activity, we took steps to secure our email system and launched an investigation with the assistance of a leading digital forensics firm to determine what happened and whether personal information may have been accessed or acquired without authorization.

The investigation revealed that one Columbia College employee email account had been accessed without authorization on March 15, 2021. We then conducted a comprehensive review of the contents of the account to determine what data might have been involved. We determined that the account contained some of your personal information. We then worked diligently to identify up-to-date address information to notify impacted individuals which was completed on October 22, 2021. Importantly, Columbia College is not aware of any misuse of your personal information as a result of this incident.

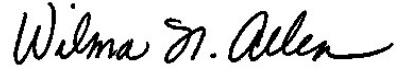
**What Information Was Involved?** The information involved may have included your name, <<variable text 1>>.

**What We Are Doing.** As soon as we discovered this incident, we took the measures referenced above and took steps to help prevent a similar incident from occurring in the future. In addition, we reported this matter to law enforcement and will provide whatever assistance is necessary to hold the perpetrator(s) of this incident accountable. Finally, out of an abundance of caution, we are offering you complimentary identity protection services through IDX, a data security and recovery services expert. Your complimentary one-year enrollment in IDX identity protection includes: credit and CyberScan monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed identity theft recovery services. Additional information about these services is included with this letter.

**What You Can Do.** Please read the recommendations included with this letter which you can follow to help protect your personal information. You can also enroll in the IDX identity protection services being provided to you, at no cost, through IDX. To enroll, please visit the IDX website at <https://app.idx.us/account-creation/protect> and provide your enrollment code located at the top of this page. Please note that the deadline to enroll is February 4, 2022. Additional information describing the IDX identity protection services, along with other recommendations to protect your personal information, is included with this letter.

**For More Information.** Please accept our sincere apologies for any worry or inconvenience that this may cause you. If you have any questions, please call 1-833-513-2602 Monday through Friday from 9 am to 9 pm Eastern Time, or please visit the IDX website at <https://app.idx.us/account-creation/protect> for assistance or for any additional questions you may have. Please have your enrollment code ready.

Sincerely,

A handwritten signature in black ink that reads "Wilma N. Allen". The signature is written in a cursive style with a large, prominent initial "W".

Wilma Allen

Vice President of Finance & Administration

## Steps You Can Take to Further Protect Your 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 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:

<b>TransUnion</b> P.O. Box 1000 Chester, PA 19016 1-800-916-8800 <a href="http://www.transunion.com">www.transunion.com</a>	<b>Experian</b> P.O. Box 2002 Allen, TX 75013 1-888-397-3742 <a href="http://www.experian.com">www.experian.com</a>	<b>Equifax</b> P.O. Box 740241 Atlanta, GA 30374 1-866-349-5191 <a href="http://www.equifax.com">www.equifax.com</a>	<b>Free Annual Report</b> P.O. Box 105281 Atlanta, GA 30348 1-877-322-8228 <a href="http://annualcreditreport.com">annualcreditreport.com</a>
---	---	--	---

**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 90 days. 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:** Under U.S. law, 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.

<b>Federal Trade Commission</b> 600 Pennsylvania Ave, NW Washington, DC 20580 <a href="http://consumer.ftc.gov">consumer.ftc.gov</a> , and <a href="http://www.ftc.gov/idtheft">www.ftc.gov/idtheft</a> 1-877-438-4338	<b>Maryland Attorney General</b> 200 St. Paul Place Baltimore, MD 21202 <a href="http://oag.state.md.us">oag.state.md.us</a> 1-888-743-0023	<b>New York Attorney General</b> Bureau of Internet and Technology Resources 28 Liberty Street New York, NY 10005 1-212-416-8433
<b>North Carolina Attorney General</b> 9001 Mail Service Center Raleigh, NC 27699 <a href="http://ncdoj.gov">ncdoj.gov</a> 1-877-566-7226	<b>Rhode Island Attorney General</b> 150 South Main Street Providence, RI 02903 <a href="http://www.riag.ri.gov">http://www.riag.ri.gov</a> 1-401-274-4400	<b>Washington D.C. Attorney General</b> 441 4th Street, NW Washington, DC 20001 <a href="http://oag.dc.gov">oag.dc.gov</a> 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 [files.consumerfinance.gov/f/201504\\_cfpb\\_summary\\_your-rights-under-fcra.pdf](https://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf).



## **One-Year Enrollment in IDX Identity Protection**

**Website and Enrollment.** Please visit <https://app.idx.us/account-creation/protect> and follow the instructions for enrollment using your Enrollment Code included with this letter.

**Activate the credit monitoring** provided as part of your IDX membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.

**Telephone.** Contact IDX at **1-833-513-2602** to speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

### **This IDX enrollment will include one-year enrollment into:**

**SINGLE BUREAU CREDIT MONITORING** - Monitoring of credit bureau for changes to the member's credit file such as new credit inquires, new accounts opened, delinquent payments, improvements in the member's credit report, bankruptcies, court judgments and tax liens, new addresses, new employers, and other activities that affect the member's credit record.

**CYBERSCAN™** - Dark Web monitoring of underground websites, chat rooms, and malware, 24/7, to identify trading or selling of personal information like SSNs, bank accounts, email addresses, medical ID numbers, driver's license numbers, passport numbers, credit and debit cards, phone numbers, and other unique identifiers.

**IDENTITY THEFT INSURANCE** - Identity theft insurance will reimburse members for expenses associated with restoring their identity should they become a victim of identity theft. If a member's identity is compromised, the policy provides coverage for up to \$1,000,000, with no deductible, from an A.M. Best "A-rated" carrier. Coverage is subject to the terms, limits, and/or exclusions of the policy.

**FULLY-MANAGED IDENTITY RECOVERY** - IDX fully-managed recovery service provides restoration for identity theft issues such as (but not limited to): account creation, criminal identity theft, medical identity theft, account takeover, rental application, tax fraud, benefits fraud, and utility creation. This service includes a complete triage process for affected individuals who report suspicious activity, a personally assigned IDX Specialist to fully manage restoration of each case, and expert guidance for those with questions about identity theft and protective measures.