

EXHIBIT 1

This notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, Black Hawk College does not waive any rights or defenses regarding the applicability of Maine law, the applicability of the Maine data event notification statute, or personal jurisdiction.

Nature of the Data Event

On October 11, 2021, Black Hawk College was notified of an incident experienced by Consociate, Inc. d/b/a Consociate Health (“Consociate”) that may impact personal information of Black Hawk College employees. Consociate is an employee benefits administrator that provides employee benefits programs and plan administrative services to Black Hawk College.

On or about January 14, 2021, Consociate learned of unusual activity within its network environment. In response, Consociate took immediate steps to secure its systems. Consociate then promptly began an investigation into this activity. In so doing, Consociate engaged leading, independent cybersecurity experts to help with its response to, and investigation of, the unusual activity identified. Through this investigation, on February 9, 2021, Consociate learned that certain locally-stored files from a segregated file server may have been accessed or acquired without authorization. Consociate’s core claims processing systems or platforms were not impacted.

On July 8, 2021, Consociate learned that the potentially impacted data contained information relating to individuals associated with certain of its business partners. Consociate then worked diligently to evaluate potentially impacted data elements, confirm identities of potentially impacted individuals, identify missing address information for potentially impacted individuals, and determine associated business partners for purposes of notifying of this incident. That process was completed on August 18, 2021. Consociate then worked diligently to notify its partners, including Black Hawk College of this incident.

Consociate notified Black Hawk College on October 11, 2021. Since then, Consociate and Black Hawk College have been working to identify current mailing addresses in order to notify individuals whose information was identified within the potentially impacted files. Consociate has no evidence that any potentially impacted information was misused.

The information that could have been subject to unauthorized access includes name, address, date of birth, Social Security number, and health insurance number.

Notice to Maine Residents

Black Hawk College directed Consociate to provide notice to affected individuals on its behalf. On or about November 3, 2021, Consociate, on Black Hawk College’s behalf, provided written notice of this incident to affected individuals, which includes approximately two (2) Maine residents. Written notice is being provided in substantially the same form as the letter attached here as *Exhibit A*.

Other Steps Taken and To Be Taken

Upon receiving Consociate's notice, Black Hawk College began an independent investigation regarding the incident. Black Hawk College reviewed the information Consociate provided to confirm the substance of the accessible data and to identify contact information for potentially affected individuals. Black Hawk College completed that effort on or about October 29, 2021.

Black Hawk College requested that Consociate provide access to credit monitoring services for twelve (12) months through Kroll to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, Black Hawk College is providing impacted individuals with guidance on how to better protect against identity theft and fraud, including advising individuals to report any suspected incidents of identity theft or fraud to their credit card company and/or bank. Black Hawk College is providing individuals with information on how to place a fraud alert and security freeze on one's credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud.

EXHIBIT A



<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country>>

Re: Notice of Data Security Incident

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

I am writing to inform you of a data security incident experienced by Consociate, Inc. d/b/a Consociate Health (“Consociate”), an employee benefits administrator that partnered with <<b2b_text_1(Business Partner)>> to provide employee benefits programs and plan administration services, which may have impacted your personal / protected health information. Consociate takes the privacy and security of all information within its possession very seriously. This letter contains information about the incident and about steps that you can take to help protect your potentially impacted information.

What Happened? On January 14, 2021, Consociate learned of unusual activity within its network environment. In response, Consociate took immediate steps to secure its systems. Consociate then promptly began an investigation into this activity. In so doing, Consociate engaged leading, independent cybersecurity experts to help with its response to, and investigation of, the unusual activity identified. Through this investigation, on February 9, 2021, Consociate learned that certain locally-stored files from a segregated file server may have been accessed or acquired without authorization. Consociate’s core claims processing systems / platforms were not impacted.

On July 8, 2021, Consociate learned that the potentially impacted data contained information relating to individuals associated with certain of its business partners. Consociate then worked diligently to evaluate potentially impacted data elements, confirm identities of potentially impacted individuals, identify missing address information for potentially impacted individuals, and determine associated business partners for purposes of notifying of this incident. That process was completed on August 18, 2021. Consociate then worked diligently to notify <<b2b_text_1(Business Partner)>> of this incident. Since then, Consociate has worked to identify current mailing addresses in order to notify individuals whose information was identified within the potentially impacted files. **Consociate has no evidence that any potentially impacted information has been misused.**

What Information Was Involved? The following information may have been potentially involved in the incident: <<b2b_text_2(Name, Impacted, Data)>>.

What Are We Doing? As soon as this incident was discovered, Consociate immediately took the steps described above and took affirmative steps to minimize the likelihood of a similar incident occurring in the future. Consociate also reported the incident to the Federal Bureau of Investigation and will provide any cooperation necessary to hold the perpetrators accountable. Further, Consociate is providing you with information about steps that you can take to help protect your information.

Although Consociate has no evidence that any potentially impacted information has been misused, out of an abundance of caution, Consociate has arranged for you to receive an offer of identity monitoring services through Kroll. Instructions to activate the complimentary One-Year Identity Monitoring Service are included here.

Visit <https://enroll.krollmonitoring.com> to activate and take advantage of your identity monitoring services.

You have until <<b2b_text_3(Activation Deadline)>> to activate your identity monitoring services.

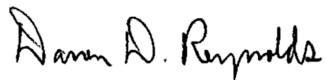
Membership Number: <<Membership Number s_n>>

What You Can Do: Consociate recommends that you follow the recommendations on the enclosed page titled “Steps You Can Take to Further Protect Your Information” and that you contact Kroll with any questions and to activate your free identity monitoring services offered to you.

For More Information: Further information about how to protect your information appears on the following page. If you have questions concerning this incident, please contact Kroll representatives by calling 1-???-???-????, Monday-Friday from 8:00 AM – 5:30 PM Central Time.

The security of your information is a top priority for Consociate, and we are committed to safeguarding your data and privacy. We regret any worry or inconvenience that this may cause you.

Sincerely,



Darren Reynolds
President and CEO
Consociate Health, Inc.

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://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf>.



TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You have been provided with access to the following services from Kroll:

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge.

To receive credit 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.