

BakerHostetler

June 4, 2020

RECEIVED

JUN 05 2020

CONSUMER PROTECTION

Baker & Hostetler LLP

2929 Arch Street
Cira Centre, 12th Floor
Philadelphia, PA 19104-2891

T 215.568.3100
F 215.568.3439
www.bakerlaw.com

Eric A. Packel
direct dial: 215.564.3011
epackel@bakerlaw.com

VIA OVERNIGHT MAIL

Attorney General Gordon MacDonald
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

Re: Security Incident Notification

Dear Attorney General MacDonald:

We are writing on behalf of our client, St. Michael's College ("SMC"), to notify your office of a security incident involving 21 residents of New Hampshire.

SMC's investigation of a phishing email incident recently determined that an unauthorized party could have accessed personal information contained in some SMC employee email accounts. Upon learning of the incident, SMC promptly secured the email accounts and a leading cyber security firm was engaged to assist with the investigation. The investigation determined that an unauthorized actor may have accessed the employee email accounts between the dates of November 13, 2019 and December 3, 2019. The investigation was not able to determine which emails or attachments, if any, were viewed by the unauthorized actor. SMC then conducted a comprehensive review of the contents of the email accounts and determined on, April 16, 2020, that an email or attachment contained the personal information of 21 residents of New Hampshire, including names and Social Security numbers.

On June 4, 2020, SMC mailed written notifications to the potentially affected residents of New Hampshire in accordance with N.H. Rev. Stat. § 359-C:20 in substantially the same form as the enclosed letter.¹ SMC is offering a complimentary one-year membership in credit monitoring and identity theft protection services through Experian. SMC is also providing a telephone

¹ SMC, through this report, does not waive its objection that New Hampshire lacks personal jurisdiction over SMC.

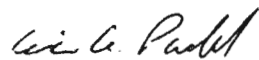
June 4, 2020
Page 2

number for potentially affected individuals to call with any questions they may have about the incident.

To help prevent an incident like this from happening in the future, SMC is providing additional training to its employees regarding phishing emails and implementing additional technical cybersecurity measures.

Please do not hesitate to contact me if you have any questions regarding this matter.

Sincerely,



Eric A. Packel
Partner

Attachment



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

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

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

St. Michael's College ("SMC") is committed to protecting the information it maintains. We are writing to inform you that we recently identified and addressed a security incident that may have involved your information. This notice explains the incident, measures we have taken, and some steps you can take in response.

Our investigation of a phishing email incident recently determined that an unauthorized party could have accessed information of yours contained in some SMC employee email accounts. Upon learning of the incident, we promptly secured the email accounts and a leading cyber security firm was engaged to assist with the investigation. Our investigation determined that an unauthorized actor may have accessed the employee email accounts between the dates of November 13, 2019 and December 3, 2019. The investigation was not able to determine which emails or attachments, if any, were viewed by the unauthorized actor. On February 17, 2020, we determined that the email accounts might contain personal information. Out of an abundance of caution, we then conducted a comprehensive review of the contents of the email accounts and determined, on April 16, 2020, that an email or attachment contained your <<b2b_text_3(ImpactedData)>>.

Although, to date, we have no evidence that your information has been misused, we assure you that we take this incident very seriously. We encourage you to remain vigilant by reviewing your account statements and credit reports for any unauthorized activity. As a precaution, we are offering you a complimentary one-year membership in Experian's® IdentityWorksSM Credit 3B. This product helps detect possible misuse of your personal information and provides you with identity protection services focused on immediate identification and resolution of identity theft. IdentityWorks Credit 3B is completely free to you and enrolling in this program will not hurt your credit score. For more information on IdentityWorks Credit 3B, including instructions on how to activate your complimentary membership as well as some additional steps you can take to help protect yourself, please see the additional information provided with this letter.

We regret any inconvenience or concern this may cause you. To help prevent an incident like this from happening in the future, we are providing additional training to our employees regarding phishing emails and implementing additional technical cybersecurity measures.

If you have any questions, please call 1-844-975-2611 Monday through Friday between the hours of 9:00 a.m. and 6:30 p.m., Eastern Time.

Sincerely,

William O Anderson

William O Anderson
Chief Information Officer

ADDITIONAL DETAILS REGARDING YOUR 12-MONTH EXPERIAN IDENTITYWORKS CREDIT 3B MEMBERSHIP

While Identity Restoration assistance is immediately available to you, we also encourage you to activate the fraud detection tools available through Experian IdentityWorksSM as a complimentary one-year membership. This product provides you with identity detection and resolution of identity theft. To start monitoring your personal information please follow the steps below:

- Ensure that you **enroll by**: <<b2b_text_1(EnrollmentDeadline)>> (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: <https://www.experianidworks.com/3bcredit>
- Provide your **activation code**: <<Member ID>>

If you have questions about the product, need assistance with enrolling or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 877-890-9332 by <<b2b_text_1(EnrollmentDeadline)>>. Be prepared to provide engagement number <<b2b_text_2(EngagementNumber)>> as proof of eligibility for the identity restoration services by Experian.

A credit card is **not** required for enrollment in Experian IdentityWorks Credit.

You can contact Experian **immediately** regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup**: See what information is associated with your credit file. Daily credit reports are available for online members only. *
- **Credit Monitoring**: Actively monitors Experian file for indicators of fraud.
- **Identity Restoration**: Identity Restoration agents are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™**: You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **\$1 Million Identity Theft Insurance****: Provides coverage for certain costs and unauthorized electronic fund transfers.

What you can do to protect your information: There are additional actions you can consider taking to reduce the chances of identity theft or fraud on your account(s). Please refer to www.ExperianIDWorks.com/restoration for this information.

* Offline members will be eligible to call for additional reports quarterly after enrolling.

** Identity theft insurance is underwritten by insurance company subsidiaries or affiliates of American International Group, Inc. (AIG). The description herein is a summary and intended for informational purposes only and does not include all terms, conditions and exclusions of the policies described. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

ADDITIONAL STEPS YOU CAN TAKE

We remind you it is always advisable to be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting companies is as follows:

- *Equifax*, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111
- *Experian*, PO Box 2002, Allen, TX 75013, www.experian.com, 1-888-397-3742
- *TransUnion*, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-916-8800

If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your state. You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the Federal Trade Commission is as follows:

- *Federal Trade Commission*, Consumer Response Center, 600 Pennsylvania Avenue NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft

Fraud Alerts and Credit or Security Freezes:

Fraud Alerts: There are two types of general fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud—an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years.

To place a fraud alert on your credit reports, contact one of the nationwide credit bureaus. A fraud alert is free. The credit bureau you contact must tell the other two, and all three will place an alert on their versions of your report.

For those in the military who want to protect their credit while deployed, an Active Duty Military Fraud Alert lasts for one year and can be renewed for the length of your deployment. The credit bureaus will also take you off their marketing lists for pre-screened credit card offers for two years, unless you ask them not to.

Credit or Security Freezes: You have the right to put a credit freeze, also known as a security freeze, on your credit file, free of charge, which makes it more difficult for identity thieves to open new accounts in your name. That's because most creditors need to see your credit report before they approve a new account. If they can't see your report, they may not extend the credit.

How do I place a freeze on my credit reports? There is no fee to place or lift a security freeze. Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit reporting company. For information and instructions to place a security freeze, contact each of the credit reporting agencies at the addresses below:

- **Experian Security Freeze**, PO Box 9554, Allen, TX 75013, www.experian.com
- **TransUnion Security Freeze**, PO Box 2000, Chester, PA 19016, www.transunion.com
- **Equifax Security Freeze**, PO Box 105788, Atlanta, GA 30348, www.equifax.com

You'll need to supply your name, address, date of birth, Social Security number and other personal information.

After receiving your freeze request, each credit bureau will provide you with a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

How do I lift a freeze? A freeze remains in place until you ask the credit bureau to temporarily lift it or remove it altogether. If the request is made online or by phone, a credit bureau must lift a freeze within one hour. If the request is made by mail, then the bureau must lift the freeze no later than three business days after getting your request.

If you opt for a temporary lift because you are applying for credit or a job, and you can find out which credit bureau the business will contact for your file, you can save some time by lifting the freeze only at that particular credit bureau. Otherwise, you need to make the request with all three credit bureaus.

Additional information for residents of the following states:

Connecticut: You may contact and obtain information from your state attorney general at: *Connecticut Attorney General's Office*, 55 Elm Street, Hartford, CT 06106, 1-860-808-5318, www.ct.gov/ag

Maryland: The Address of St. Michael's College is One Winooski Park, Colchester, VT, 05439. You may contact and obtain information from your state attorney general at: *Maryland Attorney General's Office*, 200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023 / 1-410-576-6300, www.oag.state.md.us

New York: You may contact and obtain information from these state agencies: *New York Department of State Division of Consumer Protection*, One Commerce Plaza, 99 Washington Ave., Albany, NY 12231-0001, 518-474-8583 / 1-800-697-1220, <http://www.dos.ny.gov/consumerprotection>; and *New York State Office of the Attorney General*, The Capitol, Albany, NY 12224-0341, 1-800-771-7755, <https://ag.ny.gov>

North Carolina: You may contact and obtain information from your state attorney general at: *North Carolina Attorney General's Office*, 9001 Mail Service Centre, Raleigh, NC 27699, 1-919-716-6000 / 1-877-566-7226, www.ncdoj.gov

Rhode Island: This incident involves fifty (50) individuals in Rhode Island. Under Rhode Island law, you have the right to file and obtain a copy of a police report. You also have the right to request a security freeze, as described above. You may contact and obtain information from your state attorney general at: *Rhode Island Attorney General's Office*, 150 South Main Street, Providence, RI 02903, 1-401-274-4400, www.riag.ri.gov

West Virginia: You have the right to ask that nationwide consumer reporting agencies place "fraud alerts" in your file to let potential creditors and others know that you may be a victim of identity theft, as described above. You also have a right to place a security freeze on your credit report, as described above.