

Buffalo
New York
Chicago
Washington D.C.



www.octillolaw.com

December 29, 2023

VIA EMAIL

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
Email: Idtheft@oag.state.md.us

Dear Sir or Madam:

On behalf of Bunker Hill Community College ("BHCC"), and pursuant to the Personal Information Protection Act ("PIPA"), Md. CodeAnn. Comm. Law 14-3504, this letter provides notice of a recent data security incident. By providing this notice, BHCC does not waive any rights or defenses regarding the applicability of Maryland law, including the applicability of the Maryland data notification laws or personal jurisdiction.

On May 23, 2023, BHCC detected irregular activity on certain BHCC systems that was consistent with a ransomware attack. BHCC immediately responded to the situation by taking the affected systems offline, contacting law enforcement, and engaging data security and privacy experts to conduct an investigation.

While BHCC's investigation was ongoing, on August 18, 2023, BHCC issued a public notice of the incident, including a press release and notice on BHCC's website, which notified the BHCC community of the incident and advised them to monitor their accounts for any suspicious activity.

BHCC's investigation has since concluded that an unauthorized actor gained access to BHCC's network before deploying ransomware. The investigation also found indications that the unauthorized actor may have copied a limited amount of data from BHCC's network. Accordingly, BHCC reviewed all the relevant data to determine whether any personal information was present so it could notify individuals as appropriate. There is currently no indication that the unauthorized actor has misused any personal information for identity theft or fraud in connection with this incident.

Upon becoming aware of the unauthorized activity, BHCC immediately implemented measures to further improve the security of BHCC's information technology systems and practices, including resetting and strengthening passwords, implementing new network security tools, and adopting new network access policies. BHCC worked with leading cybersecurity experts to aid in their investigation and response, and BHCC reported this incident to relevant government agencies and law enforcement.

BHCC has determined that the incident involved the personal information of 229 Maryland residents.

BHCC's investigation determined that the following general categories of information may have been involved in the incident but are not relevant to every individual: name, date of birth, Social Security Number, driver's license number, state identification number, U.S. alien identification number, passport number, financial account number in combination with routing number, credit/debit card number, username and password, medical information, and health insurance information. Again, the circumstances are different for each individual and not every category applies to each individual. BHCC is providing written notification to impacted individuals, which includes an offer for twenty-four (24) months of cost-free credit monitoring. This notification is being sent to impacted residents via regular mail starting today, December 29, 2023. A sample copy of that individual notice is attached for your review.

For any affected individuals that BHCC does not have contact information, BHCC is providing substitute notice, including a post on BHCC's website and a press release that include details on how those individuals can confirm whether their information was involved and enroll in the credit monitoring services.

Please feel free to contact me with any questions at (716) 898-2102 or dgreene@octillolaw.com.

Sincerely,

OCTILLO

A handwritten signature in black ink, appearing to read 'D. Greene', with a stylized flourish extending to the right.

Daniel P. Greene, Esq.

Certified Information Privacy Professional, United States (CIPP/US)

Certified Information Privacy Professional, Europe (CIPP/E)

Encl.



Secure Processing Center
20 Oser Ave
Suite 100
Hauppauge, NY 11788

<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<City>><<State>><<Zip>>

<<Date>>

<<NOTICE OF DATA BREACH [CA ONLY]>>

Dear <<Name 1>>,

We are writing to inform you that Bunker Hill Community College (“BHCC” or “we”) experienced a data incident in May 2023 (“Incident”) that potentially involved your personal information (“Information”). This letter provides you with information about this Incident, our response, and if necessary, information on where to direct your questions. Additionally, we have also provided steps you can take to protect your Information, including the ability to enroll in credit monitoring services that we are offering free of charge for twenty-four (24) months.

What Happened?

On May 23, 2023, we detected irregular activity on certain BHCC systems that was consistent with a ransomware attack. BHCC immediately responded to the situation by taking the affected systems offline, engaging data security and privacy experts, contacting law enforcement, and simultaneously beginning an investigation. BHCC personnel were able to stop the unauthorized activity from spreading and contained the Incident to a limited number of BHCC systems.

The investigation found that an unauthorized actor gained access to BHCC’s network before deploying ransomware. The investigation was also able to confirm that a limited amount of data was copied from BHCC’s network. Accordingly, BHCC reviewed the relevant data to confirm the identities of individuals whose Information was potentially involved and gather contact information, where available, to send this notification.

What Information Was Involved?

BHCC’s investigation determined that the copied data included the following categories of your Information: name and <<DATA ELEMENTS>>.

What We Are Doing.

Upon becoming aware of the unauthorized activity, BHCC immediately implemented measures to further improve the security of BHCC’s information technology systems and practices, including resetting and strengthening passwords, implementing new network security tools, and adopting new network access policies. BHCC worked with leading cybersecurity experts to aid its investigation and response, and BHCC reported this Incident to relevant government agencies and law enforcement.

We are also offering a complimentary twenty-four (24)-month membership in Experian IdentityWorks as an additional option to help protect your Information. This product will provide you with industry-leading identity detection and identity theft resolution. To activate your membership and start monitoring your personal information, please follow the steps below, using the unique code assigned to you:

- You must enroll by **03/18/2024** (Your code will not work after this date.)
- Visit the Experian IdentityWorks website to enroll: <https://www.experianidworks.com/3bcredit>
- Provide your activation code: <<**Activation Code**>>

If you have questions about the product, need assistance with identity restoration, or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 800-459-5028 by March 18, 2024. If you do call Experian, please be prepared to provide engagement number **B112660** as proof of eligibility for the identity restoration services by Experian.

What You Can Do.

We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity and to detect errors.

You can also enroll in the credit monitoring services that we are offering at no cost to you.

Other Important Information.

Please review the "Information about Identity Theft Protection" section included with this letter, which provides additional information about steps you can take to protect your Information.

For More Information.

We take this Incident and the security of information in our care seriously. If you have additional questions, you may call our toll-free assistance line at 888-722-9207, Monday through Friday, 9 AM to 9 PM Eastern Time.

Sincerely,



John K. Pitcher
Vice President & CFO
Office of Administration & Finance

Encl.

INFORMATION ABOUT IDENTITY THEFT PROTECTION

Contact information for the three nationwide credit reporting agencies:

Equifax, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111

Experian, PO Box 2104, Allen, TX 75013, www.experian.com, 1-888-397-3742

TransUnion, PO Box 2000, Chester, PA 19022, www.transunion.com, 1-800-888-4213

Free Credit Report. It is recommended that you remain vigilant against incidents of fraud and identity theft by reviewing account statements and monitoring your credit report for unauthorized activity. You may obtain a copy of your credit report, free of charge, once every twelve (12) months from each of the three nationwide credit reporting agencies.

To order your annual free credit report please visit www.annualcreditreport.com or call toll free at 1-877-322-8228.

You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available from the U.S. Federal Trade Commission's ("FTC") website at www.consumer.ftc.gov) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

Fraud Alert. You may place a fraud alert in your file by calling one of the three nationwide credit reporting agencies above. A fraud alert tells creditors to follow certain procedures, including contacting you before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit.

Security Freeze. Pursuant to 15 U.S.C. § 1681c-1, you may obtain a security freeze on your credit report, free of charge, to protect your privacy and ensure that credit is not granted in your name without your knowledge. You may also submit a declaration of removal to remove information placed in your credit report as a result of being a victim of identity theft. You have a right to place a security freeze on your credit report, free of charge, or submit a declaration of removal pursuant to the Fair Credit Reporting and Identity Security Act.

The security freeze will prohibit a consumer reporting agency from releasing any information in your credit report without your express authorization or approval. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. When you place a security freeze on your credit report, you will be provided with a personal identification number, password, or similar device to use if you choose to remove the freeze on your credit report or to temporarily authorize the release of your credit report to a specific party or parties or for a specific period of time after the freeze is in place.

To place a security freeze on your credit report, you may be able to use an online process, an automated telephone line, or a written request to any of the three credit reporting agencies listed above. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, and display your name, current mailing address, and the date of issue.

Federal Trade Commission and State Attorneys General Offices. 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 home state. You may also contact these agencies for information on how to prevent or avoid identity theft.

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

For California and Wyoming Residents: This notification was not delayed as a result of any law enforcement investigation.

For Colorado Residents: You can obtain information from the federal trade commission and the credit reporting agencies about fraud alerts and security freezes.

For District of Columbia Residents: You can obtain information about steps to take to avoid identity theft from the Federal Trade Commission (contact information above) and The District of Columbia Office of the Attorney General, 400 6th Street NW, Washington, D.C. 20001, consumer.protection@dc.gov, <https://oag.dc.gov/> (202) 442-9828.

For Illinois Residents: You can obtain information from the credit reporting agencies and the Federal Trade Commission about fraud alerts and security freezes (contact information above).

For Iowa Residents: You are advised to report suspected incidents of identity theft to your local law enforcement or the Iowa Office of the Attorney General, 1305 E. Walnut Street, Des Moines IA 50319, consumer@ag.iowa.gov, 1-888-777-4590.

For Maryland Residents: You may obtain information about steps you can take to avoid identity theft from the Federal Trade Commission (contact information above) and the Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, <https://www.marylandattorneygeneral.gov/Pages/CPD/default.aspx>, 1-888-743-0023.

For Massachusetts Residents: You have the right to obtain a police report if you are a victim of identity theft.

For New Mexico Residents: Consumers have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in their credit file has been used against them, the right to know what is in their credit file, the right to ask for their credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to consumers' files is limited; consumers must give consent for credit reports to be provided to employers; consumers may limit "prescreened" offers of credit and insurance based on information in their credit report; and consumers may seek damages from violators. Consumers may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active-duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage consumers to review their rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For New York Residents: You may obtain information regarding security breach response and identity theft prevention and protection information from the Federal Trade Commission (contact information above) and the New York Office of the Attorney General, Office of the Attorney General, The Capitol, Albany, NY 12224-0341, <https://ag.ny.gov>, 1-800-771-7755.

For North Carolina Residents: You may obtain information about preventing identity theft from the Federal Trade Commission (contact information above) and the North Carolina Office of the Attorney General, Consumer Protection Division, 9001 Main Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov, 1-877-566-7266.

For Oregon Residents: You are advised to report any suspected identity theft to law enforcement, the Federal Trade Commission, and the Oregon Office of the Attorney General, 1162 Court Street NE, Salem, OR 97301, www.doj.state.or.us/, (503) 378-6002.

For Rhode Island Residents: You may obtain information about fraud alerts and security freezes from the credit reporting agencies (contact information above) and the Rhode Island Office of the Attorney General, 150 South Main Street, Providence, Rhode Island, 02903, <https://riag.ri.gov/> (401) 274-4400. You have the right to file or obtain any police report in regard to this incident.