McDonald Hopkins
A business advisory and advocacy law firm®

McDonald Hopkins LLC
300 N. LaSalle Street
Suite 1400
Chicago, IL 60654

P 1.312.280.0111
F 1.312.280.8232

Blair L. Dawson, JD, MS CyS, FIP, CIPP/US, CIPP/E, CIPM
Direct Dial: 312-642-6131
E-mail: bdawson@mcdonaldhopkins.com

June 4, 2024

VIA EMAIL (Idtheft@oag.state.md.us)

Office of the Maryland Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202

Re: Bayonne Board of Education – Incident Notification

Dear Attorney General Brown:

McDonald Hopkins PLC represents Bayonne Board of Education ("Bayonne"), located at 669 Avenue A, Bayonne, NJ 07002, regarding a recent security incident. I am writing to provide notification of an incident at Bayonne that may affect the security of personal information of approximately six (6) Maryland residents. Bayonne investigation is ongoing, and this notification will be supplemented with any new or significant facts or findings subsequent to this submission, if any. By providing this notice, Bayonne does not waive any rights or defenses regarding the applicability of Maryland law or personal jurisdiction.

On or about November 19, 2023, Bayonne became aware of potentially unauthorized access to their network due to a ransomware cybersecurity incident. Upon learning of this issue, Bayonne immediately contained the threat by disabling all unauthorized access to the network and commenced a prompt and thorough investigation. As part of the investigation, Bayonne has been working very closely with external cybersecurity professionals experienced in handling these types of incidents. The forensic investigatory team determined that the unauthorized party potentially accessed or removed data from the Bayonne environment. Subsequently, Bayonne conducted a thorough and detailed manual review of all the data contained on the impacted servers. Bayonne determined on May 9, 2024 that personal information attributable was maintained on the servers and potentially may have been accessed by the unauthorized party. The information that may have been accessed or acquired may include name and Social Security number. On May 28, 2024, Bayonne located the most recent address of the impacted individuals. Bayonne proceeded to promptly notify all potentially impacted individuals as expeditiously as possible and will be providing written notice on or about June 4, 2024. Bayonne also notified major credit reporting agencies.

As stated above, upon learning of this issue, Bayonne immediately commenced an internal investigation and promptly notified potentially affected individuals. Bayonne has no indication that the information has been used to commit financial fraud or identity theft. Bayonne wanted to inform you (and the affected residents) of the incident and to explain the steps that it is taking to help safeguard the affected residents against identity fraud. Bayonne is offering residents with Social Security numbers impacted with a complimentary membership with a credit monitoring service. Bayonne will advise the affected residents regarding precautionary measures to best protect their identity and financial accounts including: remain vigilant in reviewing financial account statements for fraudulent or irregular activity on a regular basis; the process for placing a fraud alert and/or security freeze on their credit files and obtaining free credit reports; and contact information for the consumer reporting agencies and the Federal Trade Commission. The affected residents are also being provided with the contact information for the Attorney General for Maryland. A sample of the notice letter is included herein for your reference.

At Bayonne, protecting the privacy of personal information is a top priority. Bayonne is committed to maintaining the privacy of personal information in its possession and has taken many precautions to safeguard it. Further, Bayonne continues to evaluate and improve, where appropriate, its administrative and technical safeguards including training its employees on best practices related to cybersecurity, policies, procedures, and protocols, and tools to protect its network environment.

If you have any additional questions, please contact me at (312) 642-6131 or bdawson@mcdonaldhopkins.com.

Very truly yours,

Blair L. Dawson, JD, MS CyS, FIP, CIPP/US, CIPP/E, CIPM

Encl.

[redacted]

[redacted]

June 4, 2024

IMPORTANT INFORMATION PLEASE REVIEW CAREFULLY

Dear [redacted]

The privacy and security of the personal information entrusted to us is of the utmost importance to Bayonne Board of Education. We are writing to provide you with information regarding a recent cybersecurity incident that potentially involved your personal information. Please read this notice carefully, as it provides information about the incident, the complimentary identity monitoring services we are making available to you, and the significant measures we take to protect your information.

What Happened?
On or about November 19, 2023, Bayonne detected unauthorized access to our network.

What We Are Doing.
Upon learning of the incident, we immediately took steps to secure our network and mitigate against any additional harm. In addition, we engaged external cybersecurity professionals experienced in handling these type of incidents to conduct an investigation. The forensic investigatory team learned that data potentially may have been accessed or removed by the unauthorized actor. We do not have knowledge that any information has been used to commit financial fraud or identity theft as a result of the incident, however, out of an abundance of caution, we conducted a thorough and extensive manual review of the data. After extensive efforts to identify, review, and analyze the potentially impacted data, on May 9, 2024, we determined that the impacted files contained personal information pertaining to certain individuals.

While cybersecurity threats continue to impact all of us, we are taking ever-increasing measures to protect the information entrusted to us. We continually evaluate and modify our practices and internal controls to enhance the security and privacy of your personal information. In response to this incident and through our continuing comprehensive review, we have strengthened our network and implemented additional security improvements recommended by third-party cyber security experts.

What Information Was Involved?
The information that may have been accessed contained some of your personal information, including your [redacted]

What You Can Do.

As a result of this incident, we have no evidence that any of your information has been used to commit financial fraud or identity theft. Nevertheless, out of an abundance of caution, we want to make you aware of the incident. Additionally, we are providing you with complimentary identity theft protection services with to Experian IdentityWorks[SM] for [redacted] to further protect your information. This letter also provides other precautionary measures you can take to protect your personal information, including placing a Fraud Alert and Security Freeze on your credit files and obtaining a free credit report. Additionally, you should always remain vigilant in reviewing your financial account statements and credit reports for fraudulent or irregular activity on a regular basis.

How to Enroll.

To help protect your identity, we are offering complimentary access to Experian IdentityWorks[SM] for [redacted]. Please note that Identity Restoration is available to you for [redacted] from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration. While identity restoration assistance is <u>immediately available to you</u>, we also encourage you to activate the fraud detection tools available through Experian IdentityWorks as a complimentary [redacted] membership. This product provides you with superior identity detection and resolution of identity theft. To start monitoring your personal information, please follow the steps below:

- Ensure that you **enroll by** [redacted]Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: https://www.experianidworks.com/credit
- Provide your **activation code**: [redacted]

If you have questions about the product, need assistance with Identity Restoration that arose as a result of this incident, or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at [redacted] by [redacted] Be prepared to provide engagement number [redacted] as proof of eligibility for the Identity Restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR EXPERIAN IDENTITYWORKS MEMBERSHIP

A credit card is not required for enrollment in Experian IdentityWorks. 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 specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE[TM]:** 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.

For More Information.

If you have any further questions regarding this incident, please call our dedicated and confidential toll-free response line that we have set up to respond to questions at [redacted]. The response line is available for 90 days from the date of this letter, between the hours of 9:00 a.m. to 9:00 p.m. Eastern time, Monday through Friday, excluding holidays. Please accept our apologies that this incident occurred. We are committed to maintaining the privacy of personal information in our possession and have taken many precautions to safeguard it. We continually evaluate and modify our practices and internal controls to enhance the security and privacy of your personal information.

Sincerely,
Bayonne Board of Education

---

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

** The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

– OTHER IMPORTANT INFORMATION –

1. Placing a Fraud Alert.

We recommend that you place a one-year "Fraud Alert" on your credit files, at no charge. A fraud alert tells creditors to contact you personally before they open any new accounts. To place a fraud alert, call any one of the three major credit bureaus at the numbers listed below. As soon as one credit bureau confirms your fraud alert, they will notify the others.

Equifax
P.O. Box 105069
Atlanta, GA 30348-5069
www.equifax.com/personal/credit-report-services/credit-fraud-alerts/
(888) 378-4329

Experian
P.O. Box 9554
Allen, TX 75013
www.experian.com/fraud/center.html
(888) 397-3742

TransUnion
Fraud Victim Assistance Department
P.O. Box 2000
Chester, PA 19016
www.transunion.com/fraud-alerts
(800) 680-7289

2. Consider Placing a Security Freeze on Your Credit File.

If you are very concerned about becoming a victim of fraud or identity theft, you may request a "Security Freeze" be placed on your credit file at no cost. A security freeze prohibits, with certain specific exceptions, the consumer reporting agencies from releasing your credit report or any information from it without your express authorization. You may place a security freeze on your credit report by sending a request in writing, by mail, to all three nationwide credit reporting companies. To find out more on how to place a security freeze, you can use the following contact information:

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348-5788
www.equifax.com/personal/credit-report-services/credit-freeze/
(888) 298-0045

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013
www.experian.com/freeze/center.html
(888) 397-3742

TransUnion Security Freeze
P.O. Box 160
Woodlyn, PA 19094
www.transunion.com/credit-freeze
(888) 916-8800

In order to place the security freeze, you will need to supply your name, address, date of birth, Social Security number and other personal information such as copy of a government issued identification. After receiving your freeze request, each credit reporting company will send you a confirmation letter containing 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. If you do place a security freeze prior to enrolling in a credit monitoring service, you will need to remove the freeze in order to sign up for the credit monitoring service. After you sign up for the credit monitoring service, you may refreeze your credit file.

3. Obtaining a Free Credit Report.

Under federal law, you are entitled to one free credit report every 12 months from each of the above three major nationwide credit reporting companies. Call **1-877-322-8228** or request your free credit reports online at **www.annualcreditreport.com**. Once you receive your credit reports, review them for discrepancies. Identify any accounts you did not open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting company.

4. Additional Helpful Resources.

Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Checking your credit report periodically can help you spot problems and address them quickly. If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call your local law enforcement agency and file a police report. Be sure to obtain a copy of the police report, as many creditors will want the information it contains to absolve you of the fraudulent debts. You may also file a complaint with the FTC by contacting them on the web at www.ftc.gov/idtheft, by phone at 1-877-IDTHEFT (1-877-438-4338), or by mail at Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580. Your complaint will be added to the FTC's Identity Theft Data Clearinghouse, where it will be accessible to law enforcement for their investigations. In addition, you may obtain information from the FTC about fraud alerts and security freezes.

Iowa Residents: You may contact law enforcement or the Iowa Attorney General's Office to report suspected incidents of identity Theft: Office of the Attorney General of Iowa, Consumer Protection Division, Hoover State Office Building, 1305 East Walnut Street, Des Moines, IA 50319, www.iowaattorneygeneral.gov, Telephone: 515-281-5164.

Maryland Residents: You may obtain information about avoiding identity theft from the Maryland Attorney General's Office: Office of the Attorney General of Maryland, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, www.marylandattorneygeneral.gov, Telephone: 888-743-0023.

Massachusetts Residents: Under Massachusetts law, you have the right to obtain a police report in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

New Mexico residents: You have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit. In addition, you have the right to obtain a security freeze (as explained above) or submit a declaration of removal. You have a right to bring a civil action against a consumer reporting agency that violates your rights under the Fair Credit Reporting and Identity Security Act. For more information about the FCRA, please visit www.consumer.ftc.gov/sites/default/files/articles/pdf/pdf-0096-fair-credit-reporting-act.pdf or www.ftc.gov.

New York Residents: You may obtain information about preventing identity theft from the New York Attorney General's Office: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; ag.ny.gov/consumer-frauds-bureau/identity-theft; Telephone: 800-771-7755.

North Carolina Residents: You may obtain information about preventing identity theft from the North Carolina Attorney General's Office: Office of the Attorney General of North Carolina, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 877-566-7226 (Toll-free within North Carolina), 919-716-6000.

Oregon Residents: You may obtain information about preventing identity theft from the Oregon Attorney General's Office: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us, Telephone: 877-877-9392**.**

Rhode Island Residents: You have the right to obtain a police report if one was filed, or alternatively, you can file a police report. Further, you can obtain information from the Rhode Island Office of the Attorney General about steps you can take to help prevent identity theft. You can contact the Rhode Island Attorney General at: 150 South Main Street, Providence, RI 02903, (401) 274-4400, www.riag.ri.gov. As noted above, you have the right to place a security freeze on your credit report at no charge, but note that consumer reporting agencies may charge fees for other services. To place a security freeze on your credit report, you must send a request to each of the three major consumer reporting agencies: Equifax, Experian, and TransUnion. These agencies can be contacted using the contact information provided above. In order to request a security freeze, you may need to provide the following information: your full name (including middle initial as well as Jr., Sr., II, III, etc.); Social Security number; date of birth; complete address; prior addresses; proof(s) of identification (state driver's license or ID card, military identification, birth certificate, etc.); and if you are a victim of identity theft, a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft. When you place a security freeze on your credit report, within five (5) business days you will be provided with a personal identification number or password to use if you choose to remove the freeze on your credit report or to temporarily authorize the release of your credit report for a specific period of time after the freeze is in place. To provide that authorization, you must contact the consumer reporting agency and provide all of the following: (1) the unique personal identification number or password provided by the consumer reporting agency; (2) proper identification to verify your identity; and (3) the proper information regarding the period of time for which the report shall be available to users of the credit report. There were 2 Rhode Island residents impacted.

Washington D.C. Residents: You may obtain information about preventing identity theft from the Office of the Attorney General for the District of Columbia, 400 6th Street NW, Washington D.C. 20001, oag.dc.gov/consumer-protection, Telephone: 202-442-9828.