WILSON ELSER
WILSON ELSER MOSKOWITZ EDELMAN & DICKER LLP

November 22, 2019

David H. Potter
312.821.6106 (direct)
David.Potter@wilsonelser.com

Attorney General Gordon MacDonald
Office of the New Hampshire Attorney General
33 Capitol Street
Concord, NH 03302

Re: Data Security Incident

Dear Attorney General MacDonald:

We represent KIPP DC Public Charter Schools ("KIPP DC") located in Washington, DC with respect to a potential data security incident described in more detail below. KIPP DC is a non-profit network of high-performing, college-preparatory public charter schools. KIPP DC takes the security and privacy of the information in its control very seriously, and has taken steps to prevent a similar incident from occurring in the future.

1. Nature of the security incident.

In September of 2019, KIPP DC discovered that a small number of its employees were the victims of attempted payroll fraud. KIPP DC immediately conducted an investigation to determine how the incident occurred. NPP found evidence to suggest that a collection of email accounts was accessed without authorization. KIPP DC subsequently commenced an investigation with the independent computer forensic company to determine the nature and extent of the unauthorized access. The investigation concluded on September 24, 2019. KIPP DC determined that the incident stemmed from a spear-phishing campaign in an effort to perpetrate payroll fraud and discovered that some employees' payroll service accounts may have been accessed after receiving the phishing emails. These accounts contained individuals' names in combination with their Social Security numbers and financial account information. Apart from the attempted payroll fraud, KIPP DC has no evidence of any further misuse of anyone's personal information.

2. Number of New Hampshire residents affected.

A total of one (1) New Hampshire resident may have been potentially affected by this incident. A notification letter to this individual was mailed on November 21, 2019, by first class mail. A sample copy of the notification letter is included with this letter.

3. Steps taken.

KIPP DC takes the security and privacy of the information in its control very seriously and has taken steps to prevent a similar event from occurring in the future, as well as to protect the privacy and security of potentially impacted individuals' information. This includes implementing dual-factor authentication, changing passwords for all users, providing automatic notices to users when an email comes from an external sources, and providing increased safeguards to verify emails that ask for personal and financial information. KIPP DC is also providing potentially impacted individuals with identify theft protection and credit monitoring services for a period of twelve (12) months, at its own expense, through Experian.

4. Contact information.

KIPP DC remains dedicated 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 David.Potter@wilsonelser.com or (312) 821-6164.

Very truly yours,

Wilson Elser Moskowitz Edelman & Dicker LLP

David H. Potter

Enclosure.

KIPP DC:
PUBLIC SCHOOLS

<<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>>,

I am writing to inform you of a data security incident involving KIPP DC that may have resulted in the unauthorized access to some of your personal information. **We take the privacy and protection of your personal information seriously.** We sincerely apologize and regret any inconvenience this incident may cause. This letter contains information about what happened, steps we have taken, and the resources KIPP DC is making available to help protect your identity.

We recently learned that a small number of our employees were the victims of attempted payroll fraud. Upon learning of the attempted fraud, we conducted an internal investigation to identify how the actor was able to perpetrate the attempted fraud. We identified a collection of email accounts that may have been accessed by the actor in an effort to perpetrate the fraud. We then engaged a leading computer forensic firm to investigate the unauthorized access to email accounts.

The investigation revealed that many KIPP DC employees were targeted by phishing emails in a concerted effort to perpetrate the payroll fraud. Some employees' "Workday" accounts may have been accessed after receiving the phishing emails. After an extensive investigation to determine what information may have been accessed, we discovered that your personal information, including your name, address, financial information, and Social Security number, may have been accessible to the unauthorized party. Apart from the attempted payroll fraud, we have no evidence of anyone's information being misused.

Although we are unaware of any misuse of your personal information, to help relieve concerns and restore confidence following this incident, we have secured the services of Experian to provide identity monitoring, at no cost to you, for one year. Experian's ®IdentityWorks SM provides you with superior identity detection and resolution of identity theft. Your identity monitoring services include a Current Credit Report, Credit Monitoring, Identity Restoration, IdentityWorks ExtendCare, and $1 Million Identity Theft Insurance.

Please review the enclosed "Additional Important Information" that is included with this letter. This information described the services provided by Experian.

We take the security of all information in our control seriously, and are taking steps to prevent a similar event from occurring in the future. Those steps include implementing dual-factor authentication, changing all users' passwords, providing automatic notices to users when an email comes from an external source, and providing increased safeguards to verify emails that ask for personal and financial information.

Please know that the protection and security of your personal information is of our utmost priority, and we sincerely regret any concern or inconvenience that this matter may cause you. If you have any questions, please do not hesitate to call 1-???-???-????, Monday through Friday, 8:00 a.m. to 5:30 p.m., Central Time.

Sincerely,

Scooter Ward
Senior Director of Technology
KIPP DC Public Schools

Additional Important Information

For residents of Hawaii, Michigan, Missouri, Virginia, Vermont, and North Carolina: It is recommended by state law that you remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and monitoring your credit report for unauthorized activity.

For residents of Illinois, Iowa, Maryland, Missouri, North Carolina, Oregon, and West Virginia:

It is required by state laws to inform you that you may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report from each of the three nationwide credit reporting agencies. To order your 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 at https://www.consumer.ftc.gov/articles/0155-free-credit-reports) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

For residents of Iowa:

State law advises you to report any suspected identity theft to law enforcement or to the Attorney General.

For residents of Oregon:

State laws advise you to report any suspected identity theft to law enforcement, including the Attorney General, and the Federal Trade Commission.

For residents of Maryland, Rhode Island, Illinois, New York, and North Carolina:

You can obtain information from the Maryland and North Carolina Offices of the Attorney General and the Federal Trade Commission about fraud alerts, security freezes, and steps you can take toward preventing identity theft.

Maryland Office of the Attorney General	**Rhode Island Office of the Attorney General**	**North Carolina Office of the Attorney General**	**Federal Trade Commission**	**New York Office of the Attorney General**
Consumer Protection Division	Consumer Protection	Consumer Protection Division	Consumer Response Center	Bureau of Consumer Frauds & Protection
200 St. Paul Place	150 South Main Street	9001 Mail Service Center	600 Pennsylvania Ave, NW	The Capitol
Baltimore, MD 21202	Providence RI 02903	Raleigh, NC 27699-9001	Washington, DC 20580	Albany, NY 12224-0341
1-888-743-0023	1-401-274-4400	1-877-566-7226	1-877-IDTHEFT (438-4338)	1-800-771-7755
www.oag.state.md.us	www.riag.ri.gov	www.ncdoj.com	www.ftc.gov/idtheft	https://ag.ny.gov/consumer-frauds/identity-theft

For residents of Massachusetts:

It is required by state law that you are informed of your right to obtain a police report if you are a victim of identity theft.

For residents of all states:

Fraud Alerts: You can place fraud alerts with the three credit bureaus by phone and online with Equifax (https://assets.equifax.com/assets/personal/Fraud_Alert_Request_Form.pdf), Experian (https://www.experian.com/fraud/center.html) or TransUnion (https://www.transunion.com/fraud-alerts). 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. As of September 21, 2018, initial fraud alerts last for one year. Victims of identity theft can also get an extended fraud alert for seven years. The phone numbers for all three credit bureaus are at the bottom of this page.

Monitoring: You should always remain vigilant and monitor your accounts for suspicious or unusual activity.

Security Freeze: You also have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans, and services from being approved in your name without your consent. To place a security freeze on your credit report, you need to make a request to each consumer reporting agency. You may make that request by certified mail, overnight mail, regular stamped mail, telephone or by following the instructions found at the websites listed below. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse or a minor under the age of 16, 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, display your name and current mailing address, and the date of issue. As of September 21, 2018, it is free to place, lift, or remove a security freeze. You may also place a security freeze for children under the age of 16. You may obtain a free security freeze by contacting each of the following national consumer reporting agencies:

Equifax Security Freeze	**Experian Security Freeze**	**TransUnion (FVAD)**
P.O. Box 105788	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19022
www.freeze.equifax.com	www.experian.com/freeze	freeze.transunion.com
800-525-6285	888-397-3742	800-680-7289

More information can also be obtained by contacting the Federal Trade Commission listed above.

We have secured the services of Experian to provide identity monitoring at no cost to you for one year. Experian's® IdentityWorks℠ provides you with superior identity detection and resolution of identity theft. Your identity monitoring services include a Current Credit Report, Credit Monitoring, Identity Restoration, IdentityWorks ExtendCare, and $1 Million Identity Theft Insurance.

How to Activate Your Identity Monitoring Services

1. You must activate your identity monitoring services by **<<b2b_text_1>>**. Your Activation Code will not work after this date.
2. Visit **https://www.experianidworks.com/3bcredit** to activate your identity monitoring services.
3. Provide Your Activation Code: **<<Member ID>>**

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 1-877-288-8057 by **<<b2b_text_1>>**. Be prepared to provide engagement number **<<b2b_text_2>>** as proof of eligibility for the identity restoration services by Experian.

Additional Details Regarding Your 12-Month 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:

Triple Bureau Credit Monitoring and Single Bureau Credit Report

Experian will provide a free copy of your credit report at sign up so you can see what information is associated with your credit file. Daily credit reports are also available for online members only.

Credit Monitoring

Credit Monitoring monitors your Experian file for indicators of fraud.

Identity Restoration[1]

Experian's Identity Restoration agents are immediately available to help you address credit and non-credit related fraud.

Experian IdentityWorks ExtendCARE™

Experian will provide the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.

$1 Million Identity Fraud Loss Reimbursement

Experian provides coverage for certain costs and unauthorized electronic fund transfers.

What to Do When Your Information Has Been Fraudulently Used

If you believe there was a fraudulent use of your information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent at 1-877-288-8057.

[1] Identity Restoration support is available to you for one year 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. You will also find self-help tips and information about identity protection at this site.