MULLEN COUGHLIN LLC
ATTORNEYS AT LAW

Ryan C. Loughlin
Office: (267) 930-4786
Fax: (267) 930-4771
Email: rloughlin@mullen.law

426 W. Lancaster Avenue, Suite 200
Devon, PA 19333

December 1, 2020

VIA U.S. MAIL

Consumer Protection Bureau
Office of the New Hampshire Attorney General
33 Capitol Street
Concord, NH 03301

Re: Notice of Data Event

Dear Sir or Madam:

We represent Indianapolis Public Schools ("IPS"), located at 120 E. Walnut St., Indianapolis, IN 46204, and are writing to notify your office of an incident that may affect the security of some personal information relating to two (2) New Hampshire residents. IPS will supplement this notice with any new significant facts learned subsequent to its submission. By providing this notice, IPS does not waive any rights or defenses regarding the applicability of New Hampshire law, the applicability of the New Hampshire data event notification statute, or personal jurisdiction.

Nature of the Data Event

On or about April 19, 2020, IPS became aware of suspicious activity relating to certain IPS employee email accounts. IPS immediately launched an investigation which included working with a third-party forensic investigation firm to determine what may have happened. On May 7, 2020, the investigation confirmed that certain IPS email accounts were accessed by an unknown party. Unfortunately, the investigation was not able to determine which emails, if any, were viewed.

As IPS was unable to determine if any emails were viewed, out of an abundance of caution, IPS, through a third-party specialist, completed a programmatic and manual review to determine whether personal information may have been present in the email accounts at the time of the incident. On September 4, 2020, IPS determined certain personal information was present in

relevant email accounts. Since that time, IPS has been working to locate address information for individuals whose personal information may have been accessible within the account.

The information that could have been subject to unauthorized access includes name and Social Security number.

Notice to New Hampshire Residents

On or about December 1, 2020, IPS provided written notice of this incident to potentially affected individuals, which includes two (2) New Hampshire 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 discovering the event, IPS moved quickly to investigate and respond to the incident, assess the security of IPS systems, and notify potentially affected individuals. IPS is also working to implement additional safeguards and training to its employees. IPS is providing 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, IPS 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. IPS 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.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4786.

Very truly yours,

Ryan C. Loughlin of
MULLEN COUGHLIN LLC

RCL/acl

EXHIBIT A

Si necesita tener esta carta en español, llame al 317-226-4000 para solicitar una. Lo traducieramos y te enviaremos.

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

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

<<B2B_TEXT_2(SUBJECTLINE)>>

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

The Indianapolis Public Schools ("IPS") is writing to notify you of an incident that may affect the security of some of your personal information. We take this incident very seriously, and this letter provides details of the incident, our response, and resources available to you to help protect your information from possible misuse, should you feel it is appropriate to do so.

What Happened? On April 19, 2020, we became aware of suspicious activity relating to certain IPS employee email accounts. We immediately launched an investigation which included working with a third-party forensic investigation firm to determine what may have happened. On May 7, 2020, the investigation confirmed that certain IPS email accounts were accessed by an unknown party. Unfortunately, the investigation was not able to determine which emails, if any, were viewed.

Since we are unable to determine if any emails were viewed, we completed a programmatic and manual review to determine whether sensitive information was present in the emails at the time of the incident. On September 4, 2020, we determined your personal information was present in one of the relevant email accounts. We are providing you this notification out of an abundance of caution because your personal information was present in an email account at the time of the incident.

What Information Was Involved? Our investigation determined that the information accessible within the email accounts included your <<b2b_text_1(DataElements)>>. Please note that while our investigation did not reveal evidence that your information was actually viewed by the unauthorized actor, we are providing you this notice to ensure you are aware of this incident.

What We Are Doing? Information privacy and security are among our highest priorities. Upon learning of this incident, we quickly took steps to confirm the security of our systems, including our employee email accounts. We reset passwords for all relevant IPS email accounts and are reviewing our company policies and procedures relating to data security.

In an abundance of caution, we are notifying potentially affected individuals, including you, so that you may take further steps to help protect your personal information, should you feel it is appropriate to do so. We have arranged to have Kroll provide identity monitoring services for 12 months at no cost to you as an added precaution.

What Can You Do? You may review the information contained in the attached "Steps You Can Take to Help Protect Your Information." You may also activate the identity monitoring services we are making available to you. IPS will cover the cost of this service. Because the activation process does not allow us to activate on your behalf, you will need to activate yourself by following the instructions outlined in this letter.

For More Information. We recognize that you may have questions not addressed in this letter. If you have additional questions, please contact 1-833-971-3234, Monday through Friday, 9:00 a.m. to 6:30 p.m., Eastern Time, excluding certain national U.S. holidays.

We take the privacy and security of the personal information in our care seriously, and sincerely regret any inconvenience or concern this incident may cause you.

Sincerely,

Aleesia L. Johnson
Superintendent
Indianapolis Public Schools

Steps You Can Take to Help Protect Your Information

Activate Identity Monitoring Services:

To help relieve concerns and restore confidence following this incident, we have secured the services of Kroll to provide identity monitoring at no cost to you for one year. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

Visit **https://enroll.idheadquarters.com** to activate and take advantage of your identity monitoring services.

*You have until **February 23, 2021** to activate your identity monitoring services.*

Membership Number: <<Member ID>>

Additional information describing your services is included with this letter.

Monitor Accounts

We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity. Under U.S. law you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report.

You have the right to place a "security freeze" on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a security freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a security freeze on your credit report. Should you wish to place a security freeze, please contact the major consumer reporting agencies listed below:

Experian	**TransUnion**	**Equifax**
PO Box 9554	P.O. Box 160	PO Box 105788
Allen, TX 75013	Woodlyn, PA 19094	Atlanta, GA 30348-5788
1-888-397-3742	1-888-909-8872	1-800-685-1111
www.experian.com/freeze/center.html	www.transunion.com/credit-freeze	www.equifax.com/personal/credit-report-services

In order to request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, military identification, etc.);
7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

As an alternative to a security freeze, you have the right to place an initial or extended "fraud alert" on your file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the agencies listed below:

Experian	**TransUnion**	**Equifax**
P.O. Box 9554	P.O. Box 2000	P.O. Box 105069
Allen, TX 75013	Chester, PA 19016	Atlanta, GA 30348
1-888-397-3742	1-800-680-7289	1-888-766-0008
www.experian.com/fraud/center.html	www.transunion.com/fraud-victim-resource/place-fraud-alert	www.equifax.com/personal/credit-report-services

Additional Information

You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General.

The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.

For California Residents: Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft.

For Kentucky Residents: Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601, www.ag.ky.gov, Telephone: 1-502-696-5300.

For Maryland Residents: Office of the Attorney General of Maryland, Consumer Protection Division 200 St. Paul Place Baltimore, MD 21202, www.oag.state.md.us/Consumer, Telephone: 1-888-743-0023. IPS may be contacted by mail at 120 E. Walnut St., Indianapolis, IN 46204.

For 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 reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from a violator. You 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. You can review your 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: The Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; https://ag.ny.gov/.

For North Carolina Residents: Office of the Attorney General of North Carolina, Consumer Protection Division, 9001 Mail Service Center Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 1-919-716-6400, 877-566-7226 (toll free within NC).

For Oregon Residents: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 877-877-9392.

For Rhode Island Residents: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are <<##>> Rhode Island residents impacted by this incident.

Kroll | A Division of DUFF&PHELPS

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 will 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.