MULLEN COUGHLIN LLC
ATTORNEYS AT LAW

Carolyn Purwin Ryan
Office: (267) 930-6836
Fax: (267) 930-4771
Email: CPurwinRyan@mullen.law

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

February 4, 2021

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 the City of Philadelphia ("the City") located at 1515 Arch Street, 15th Floor, Philadelphia, PA 19102-1595, and are writing to notify your office of an incident that may affect the security of some personal information relating to one (1) New Hampshire resident. The investigation into this matter is ongoing, and this notice may be supplemented with any new significant facts learned after its submission. By providing this notice, the City 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 March 31, 2020, the City's Department of Behavioral Health and Intellectual disAbility Services ("DBHIDS") became aware of suspicious activity related to an employee of the Division of Intellectual disAbility Services' ("IDS") email account. The City quickly launched an internal investigation to determine the nature and scope of the activity, as well as the extent of potentially affected information. The investigation confirmed that the email account had been subject to unauthorized access between March 11 and March 31, 2020. Upon further investigation, the City confirmed that additional DBHIDS employees' email accounts were also subject to unauthorized access intermittently between March 11 and November 16, 2020. However, the investigation was unable to determine which, if any, emails and attachments in the accounts were viewed by the unauthorized actor. Therefore, the City began a thorough review of the contents of the accounts to determine whether they contained sensitive information and to identify all potentially impacted individuals. On December 21, 2020, the City completed its review of the IDS and other DBHIDS

employees' compromised accounts and determined that information related to a New Hampshire resident was present in at least one of these accounts during the period of unauthorized access.

The City cannot confirm specifically whether any personal information was viewed by the unauthorized actor(s). However, the investigation determined that the information present in one or more of the impacted email accounts during the period of unauthorized access may have included the following information related to a New Hampshire resident: name, account and/or medical record numbers, health insurance information, and clinical information such as diagnosis, dates of service, provider names, and description of services the individual applied for or was receiving. The impacted email accounts may have also contained certain individuals' Social Security number and/or driver's license number.

Notice to New Hampshire Resident

On or about February 4, 2021, the City is providing written notice of this incident to affected individuals, which includes one (1) New Hampshire resident. 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 learning of the incident, the City moved quickly to confirm and enhance the security of its systems, which included resetting impacted employees' email account passwords, increasing monitoring of network activity, and implementing tools to enhance email security. As described above, the City also launched an in-depth investigation to determine the full nature and scope of this incident. As part of its ongoing commitment to information privacy and security, the City is reviewing its existing policies and procedures to identify ways to better prevent similar incidents from occurring in the future.

Out of an abundance of caution, the City is providing potentially affected individuals with access to complimentary credit monitoring services for twelve (12) months through Kroll. Additionally, the City 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 to their credit card company and/or bank. Furthermore, the City 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) 930-6836.

Very truly yours,

Carolyn Purwin Ryan of
MULLEN COUGHLIN LLC

CPR:mfl

Exhibit A

CITY OF PHILADELPHIA

Department of Behavioral Health and Intellectual disAbility Services
Promoting Recovery, Resilience & Self Determination

Jill Bowen, Ph.D.
Commissioner

Roland Lamb
Deputy Commissioner

Sosunmolu Shoyinka, M.D.
Chief Medical Officer

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

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

RE: Important Security Notification
Please read this entire letter.

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>:

The City of Philadelphia (the "City") Department of Behavioral Health and Intellectual disAbility Services ("DBHIDS") is writing to inform you of a recent event that may impact the security of some of your personal information. The City has your information because you received services from the Division of Intellectual disAbility Services ("IDS"), which coordinates and administers home and community habilitation, adaptive equipment, behavior and other therapies, early intervention, and residential, respite, employment, and day services for individuals with intellectual disabilities in Philadelphia. While we are unaware of any fraudulent misuse of your personal information, we are providing you with details about the event, steps we are taking in response, and resources available to help you protect yourself from the possibility of identity theft and fraud, should you feel it is appropriate to do so.

What Happened? On March 31, 2020, DBHIDS became aware of suspicious activity related to an IDS employee's email account. The City quickly launched an internal investigation to determine the nature and scope of the activity, as well as the extent of potentially affected information. The investigation confirmed that the email account had been subject to unauthorized access between March 11 and March 31, 2020. Upon further investigation, the City confirmed that additional DBHIDS employees' email accounts were also subject to unauthorized access intermittently between March 11 and November 16, 2020. However, the investigation was unable to determine which, if any, emails and attachments in the accounts were viewed by the unauthorized actor. Therefore, the City began a thorough review of the contents of the accounts to determine whether they contained sensitive information and to identify all potentially impacted individuals. On December 21, 2020, the City completed its review of the IDS and other DBHIDS employees' compromised account and determined that information related to you was present in at least one of these accounts during the period of unauthorized access.

What Information Was Involved? The City cannot confirm specifically whether any personal information was viewed by the unauthorized actor(s). However, the investigation determined that the information present in one or more of the impacted email accounts during the period of unauthorized access may have included your name, account and/or medical record numbers, health insurance information, and clinical information such as diagnosis, dates of service, provider names, and description of services you applied for or were receiving. The impacted email accounts may have also contained your Social Security number and/or driver's license number.

What is the City Doing? The privacy of the people we serve is very important to us and we will continue to do everything we can to protect it. Upon learning of this event, we moved quickly to confirm and enhance the security of our systems, which included resetting impacted employees' email account passwords, increasing monitoring of network activity, and implementing tools to enhance email security. As described above, we also launched an in-depth investigation to determine the full nature and scope of this incident. As part of our ongoing commitment to information privacy and security, we are reviewing our existing policies and procedures to identify ways to better prevent similar incidents from occurring in the future.

Out of an abundance of caution, we are also providing you with 12 months of complimentary access to identity monitoring services through Kroll, as well as guidance on how to help protect against the possibility of information misuse. While the City is covering the cost of these services, you will need to complete the activation process yourself.

What Can You Do? You can learn more about how to protect against the possibility of information misuse in the enclosed *Steps You Can Take to Help Protect Personal Information.* There, you will also find more information about the identity monitoring services we are offering and how to activate these services.

For More Information. We understand that you may have questions about this incident that are not addressed in this letter. If you have additional questions, please call our dedicated call center, toll-free, at 1-855-763-0063, 9:00 a.m. to 6:30 p.m. Eastern Time, excluding some U.S. holidays.

We apologize for any inconvenience this incident may cause you. We remain committed to the privacy and security of information in our possession.

Sincerely,

Jill Bowen, PhD

Jill Bowen
Commissioner

Steps You Can Take to Help Protect Personal 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 **May 10, 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 explanations of benefits, 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, 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, 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 your child 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); 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 Maryland residents, the Attorney General can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, 1-410-528-8662, www.oag.state.md.us.

For North Carolina residents, the Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-566-7226 or 1-919-716-6000, www.ncdoj.gov. You can obtain information from the Attorney General or the Federal Trade Commission about preventing identity theft.

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 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. We encourage you to 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/.

ATENCIÓN: si habla español, tiene a su disposición servicios gratuitos de asistencia lingüística. Llame al 1-855-763-0063.

注意：如果您使用繁體中文，您可以免費獲得語言援助服務。請致電 1-855-763-0063.