EXHIBIT 1

We write on behalf of the City of Philadelphia ("the City") located at 1515 Arch Street, 15th Floor, Philadelphia, PA 19102-1595 in a follow up to our notice provided on June 11, 2021 to notify your office of an incident that may affect the security of certain personal information related to approximately four (4) additional Maine residents. By providing this notice, the City does not waive any rights or defenses regarding the applicability of Maine law, the Maine data breach notification statute, or personal jurisdiction.

In its previous submission to your office, the City explained that it began providing written notice to individuals whose personal information may have been impacted by a March 2020 data incident. In those notices, the City noted that the submissions to your office might be supplemented if significant facts regarding Maine residents were later learned. Since providing those notices, the City has continued its review of the affected data and determined, with assistance from its business associate, Community Behavioral Health ("CBH"), the identities and states of residence of additional individuals potentially impacted by this incident. CBH works with the City's Department of Behavioral Health and Intellectual disAbility Services ("DBHIDS") to administer the behavioral health Medicaid program ("Healthchoices") for the Philadelphia region. Although the City and CBH have now completed their reviews of the data affected by this incident, a further supplement to this notice may be filed if new or otherwise significant facts regarding Maine residents are discovered.

The information related to individuals that may have been subject to unauthorized access or acquisition varies by affected person but includes name, account and/or medical record numbers, health insurance information, clinical information such as diagnoses, dates of service, provider names, treatment costs, prescriptions, and description of services individuals applied for or were receiving. The impacted email accounts also contained certain individuals' Social Security number, driver's license number or state issued ID number, financial account information, payment card information, and/or online credentials.

On August 6, 2021, the City provided written notice of this incident to these additional individuals whose information may have been impacted. Written notice is being provided in substantially the same form as the letter attached here as ***Exhibit A***. Written notice will be provided by CBH in substantially the same form as the letter attached here as ***Exhibit B***.

EXHIBIT A

CITY OF PHILADELPHIA

OFFICE OF THE CHIEF ADMINSTRATIVE OFFICER

Stephanie Tipton
Chief Administrative Officer

1401 John F. Kennedy Blvd. - Suite 630
Philadelphia, PA 19102-1683

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

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

RE: Notice of Data Breach
Please read this entire letter.

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

The City of Philadelphia (the "City") is writing to inform you of a recent event that may impact the security of some of your personal information. While we are unaware of any misuse of your personal information, we are providing you with details about the event, steps we have taken 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, the City became aware of suspicious activity related to an 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 multiple City employees' email accounts were impacted by a phishing attack, and as a result, were subject to unauthorized access intermittently between March 11, 2020 and January 14, 2021. 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. The City completed its review of the employees' compromised accounts and determined on July 12, 2021 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 included: <<b2b_text_1(DataElements)>><<b2b_text_2(DataElementsCont)>>.

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 have updated our policies and procedures to protect against similar incidents.

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,

Stephanie Tipton
Chief Administrative Officer
City of Philadelphia

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.krollmonitoring.com** to activate and take advantage of your identity monitoring services.

*You have until **November 19, 2021** to activate your identity monitoring services.*

Membership Number: **<<Membership Number s_n>>**

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.

Consumers have the right to place an initial or extended "fraud alert" on a credit 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 three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a "credit freeze" on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer's express authorization. The credit 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 credit 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 credit freeze on your credit report. To request a security freeze, you will need to provide the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to 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.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if you are a victim of identity theft.

Should you wish to place a fraud alert or credit freeze, please contact the three major credit reporting bureaus listed below:

Equifax	**Experian**	**TransUnion**
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
888-298-0045	1-888-397-3742	833-395-6938
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000 Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160 Woodlyn, PA 19094

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); 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 District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th St NW, Washington, DC 20001; 202-727-3400; and oag@dc.gov.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and www.oag.state.md.us. The City of Philadelphia is located at 1101 Market Street, 7th Floor, Philadelphia, PA 19107-2907.

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

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 bureaus 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 Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are X Rhode Island residents impacted by this incident.

For New York residents, the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or https://ag.ny.gov/.

KROLL

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'll 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.

EXHIBIT B

Community Behavioral Health

Return to IDX
PO Box 4129
Everett WA 98204

ENDORSE
NAME
ADDRESS1
ADDRESS2
CSZ
COUNTRY
BREAK
SEQ
CODE 2D
Ver 5AGE

To Enroll, Please Call:
1-833-664-2001
Or Visit:
https://response.idx.us/cbh
Enrollment Code: <<XXXXXXXX>>

August 10, 2021

RE: Important Security Notification
Please read this entire letter.

Dear <<First Name>> <<Last Name>>:

Community Behavioral Health ("CBH") is writing to inform you of a recent event that may impact the security of some of your personal information. 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 protect you from the possibility of identity theft and fraud, should you feel it is appropriate to do so. CBH is a business associate of the City of Philadelphia (the "City")'s Department of Behavioral Health and Intellectual Disability Services ("DBHIDS"), and provides assistance to DBHIDS in administering the behavioral health Medicaid program (HealthChoices) for the Philadelphia region. In particular, although CBH does not provide direct care, CBH helps arrange and pay for behavioral health care.

What Happened? On March 31, 2020, DBHIDS became aware of suspicious activity related to an 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 multiple DBHIDS and CBH employees' email accounts were impacted by a phishing attack, and as a result, were 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 and CBH 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 March 22, 2021, the review of the CBH employees' compromised accounts concluded and it was determined that information related to CBH's clients was present in at least one of these accounts during the period of unauthorized access. Between March and July 2021, CBH retained an independent third party vendor to further review the data contained in the accounts at issue in order to identify any additional individual impacted by this incident. On July 9, 2021, the data mining exercise concluded, and it has been 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? CBH 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, date of birth, medical record number, Medicare/Medicaid number, Social Security Number, health insurance information, treatment and diagnosis information.

What We Are 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, the City 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 credit monitoring and identity restoration services through IDX, as well as guidance on how to help protect against the possibility of information misuse. While CBH is covering the cost of these services, you will need to complete the activation process on your behalf.

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

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 1-833-664-2001, Monday through Friday from 9 am - 9 pm Eastern Time, excluding 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,

Dr. Faith Dyson-Washington, Chief Executive Officer
Community Behavioral Health

Steps You Can Take to Help Protect Personal Information

Activate Identity Monitoring Services

1. Website and Enrollment. Go to https://response.idx.us/cbh and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.

2. Activate the credit monitoring provided as part of your IDX identity protection membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.

3. Telephone. Contact IDX at 1-833-664-2001 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

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
PO Box 9554
Allen, TX 75013
1-888-397-3742
www.experian.com/freeze/center.html

TransUnion
P.O. Box 160
Woodlyn, PA 19094
1-888-909-8872
www.transunion.com/credit-freeze

Equifax
PO Box 105788
Atlanta, GA 30348-5788
1-800-685-1111
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:

SEQ
CODE 2D

Experian	TransUnion	Equifax
P.O. Box 9554 Allen, TX 75013 1-888-397-3742 www.experian.com/fraud/center.html	P.O. Box 2000 Chester, PA 19016 1-800-680-7289 www.transunion.com/fraud-victim-resource/place-fraud-alert	P.O. Box 105069 Atlanta, GA 30348 1-888-766-0008 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 residents of *Hawaii, Michigan, Missouri, North Carolina, Vermont, Virginia, and Wyoming*: 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 *Colorado*, *Illinois*, *Iowa*, *Maryland*, *Missouri*, *New Mexico*, *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 *Massachusetts*: It is required by state law that you are informed of your right to obtain a police report filed 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.

For residents of *New Mexico*: State law advises you to review personal account statements and credit reports, as applicable, to detect errors resulting from the security breach.

For residents of *Oregon*: State law advises you to report any suspected identity theft to law enforcement, including the Attorney General, and the Federal Trade Commission.

For residents of *Rhode Island*: It is required by state law that you are informed of your right to file or obtain a police report in regard to this incident.

For residents of Arizona, Colorado, District of Columbia, Illinois, Maryland, New York, North Carolina,* and *Rhode Island: You can obtain information from the Offices of the Attorney General and the Federal Trade Commission about fraud alerts, security freezes, and steps you can take toward preventing identity theft.

Federal Trade Commission - Consumer Response Center: 600 Pennsylvania Ave, NW, Washington, DC 20580; 1-877-IDTHEFT (438-4338); www.identitytheft.gov

Arizona Office of the Attorney General Consumer Protection & Advocacy Section, 2005 North Central Avenue, Phoenix, AZ 85004 1-602-542-5025

Colorado Office of the Attorney General Consumer Protection 1300 Broadway, 9th Floor, Denver, CO 80203 1-720-508-6000 www.coag.gov

District of Columbia Office of the Attorney General – Office of Consumer Protection: 400 6th Street, NW, Washington, DC 20001; 202-727-3400; www.oag.dc.gov

Illinois office of the Attorney General - 100 West Randolph Street**,** Chicago, IL 60601**;** 1-866-999-5630**;** www.illinoisattorneygeneral.gov

Maryland Office of the Attorney General - Consumer Protection Division**:** 200 St. Paul Place**,** 16th floor, Baltimore, MD 21202; 1-888-743-0023; www.oag.state.md.us

New York Office of Attorney General - Consumer Frauds & Protection: The Capitol, Albany, NY 12224; 1-800-771-7755; https://ag.ny.gov/consumer-frauds/identity-theft

North Carolina Office of the Attorney General - Consumer Protection Division**:** 9001 Mail Service Center, Raleigh, NC 27699**;** 1-877-566-7226; www.ncdoj.com

Rhode Island Office of the Attorney General - Consumer Protection: 150 South Main St., Providence RI 02903**;** 1-401-274-4400**;** www.riag.ri.gov

ATENCIÓN: si habla español, tiene a su disposición servicios gratuitos de asistencia lingüística. Llame al 1-833-664-2001.

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 1-833-664-2001.

SEQ
CODE 2D