



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 that were provided or paid for by DBHIDS or its business associate, Community Behavioral Health (“CBH”). DBHIDS provides or funds a variety of services for Philadelphia residents, including: mental health and addiction services for adults and children; homeless services; and home and community habilitation, adaptive equipment, behavior and other therapies, early intervention, and residential, respite, employment, and day services for individuals with intellectual disability in the City. DBHIDS also works with CBH to administer the behavioral health Medicaid program (“Healthchoices”) for the Philadelphia region. While we are unaware of any 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 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 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 City completed its review of the 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 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 are reviewing our existing policies and procedures to identify ways to better prevent similar incidents from occurring in the future.

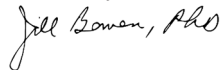
Out of an abundance of caution, we are also providing you with 12 months of complimentary access to identity monitoring services through Kroll, as well as guidance on how to help protect against the possibility of information misuse. While the City is covering the cost of these services, you will need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

A handwritten signature in cursive script that reads "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 **July 30, 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.

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 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 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/>.

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。



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

CBH LETTERHEAD

<<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>>:

Community Behavioral Health, Inc. (“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, CBH completed its review of the CBH 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? 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 is CBH 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 [Vendor Name], 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 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 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 XXX-XXX-XXXX, [insert call center hours], 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,

© 2006 The Authors
Journal compilation © 2006 Blackwell Publishing Ltd

Steps You Can Take to Help Protect Personal Information

Activate Identity Monitoring Services

[Insert credit monitoring enrollment instructions]

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:

Experian

P.O. Box 9554
Allen, TX 75013
1-888-397-3742

www.experian.com/fraud/center.html

TransUnion

P.O. Box 2000
Chester, PA 19016
1-800-680-7289

www.transunion.com/fraud-victim-resource/place-fraud-alert

Equifax

P.O. Box 105069
Atlanta, GA 30348
1-888-766-0008

www.equifax.com/personal/credit-report-services