May 16, 2024 – The City of Philadelphia (the "City") Department of Behavioral Health and Intellectual disAbility Services ("DBHIDS") is issuing updated notice of an event that may impact the security of information related to certain individuals. This notice supplements the notice previously posted on the City's website on or about October 20, 2023. We are providing updated information about the event, our response, and steps potentially affected individuals may take to better protect against the possibility of identity theft and fraud, should they feel it is appropriate to do so.

What Happened? On May 24, 2023, the City initially became aware of suspicious activity in its email environment. We launched an investigation, with the assistance of third-party cybersecurity specialists, to determine the nature and scope of the event. The investigation determined that between May 26, 2023 and July 28, 2023, an unauthorized actor may have gained access to certain City email accounts and certain information contained therein. Also, on August 22, 2023, we became aware that the at-issue email accounts include email accounts that may contain protected health information.

In an abundance of caution, we conducted a comprehensive, programmatic and manual review of the potentially impacted email accounts to determine whether personal information or protected health information was potentially affected. Once complete, we also worked to validate the results and locate missing address information. We recently completed this process and are now providing potentially affected individuals with notice of this event via written letter, by issuing updated notice to the media, and by posting this updated notice on our website.

What Information Was Affected. The types of potentially impacted information vary by individual and could include the following: name, address, date of birth, Social Security number financial account information, medical information including occupational health-related information, or health insurance information.

What We Are Doing. We take this event and information security very seriously. Upon learning of this event, we immediately took steps further secure our systems and email environment. As part of our ongoing commitment to information security, we are also reviewing our existing policies and procedures, implementing additional administrative and technical safeguards to further secure information in our care, and providing additional training on how to safeguard information in our email environment. We also reported this event to the U.S. Department of Health and Human Services and appropriate state regulators, as necessary.

What Affected Individuals Can Do. As a precautionary measure, individuals are encouraged to remain vigilant against incidents of identity theft by reviewing account statements, credit reports, and explanations of benefits forms for unusual activity and to detect errors. Any suspicious activity should be reported promptly to your insurance company, health care provider, bank, or other applicable institution. Additional information can be found below in the *Steps You Can Take to Help Protect Your Information.*

For More Information. If you have additional questions, please call our toll-free assistance line at 1-866-898-0867, Monday through Friday from 9:00 a.m. to 6:30 p.m. Eastern Time, excluding major U.S. holidays. You may also write to the City at HIPAAprivacy@phila.gov

Steps You Can Take To Help Protect Your Information

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also directly contact the three major credit reporting bureaus listed below 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 one-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 credit 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, 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
1-888-298-0045	1-888-397-3742	1-800-916-8800

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 may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state attorney general. The Federal Trade Commission may 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. 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: 441 4th St. NW #1100 Washington, D.C. 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;1-888-743-0023; and www.oag.state.md.us.

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/.

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.