EXHIBIT 1

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 four (4) Maine residents. 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 Maine law, the applicability of the Maine data event notification statute, or personal jurisdiction.

Nature of the Data Event

.

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. On May 18, 2021, the City completed its review of the employees' compromised accounts and determined that information related Maine residents 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 included the following information related to Maine residents: name, Social Security number, and driver's license/state ID number.

Notice to Maine Residents

On June 11, 2021, the City is providing written notice of this incident to affected individuals, which includes approximately four (4) Maine residents. Written notice is being provided by the City 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 updated its policies and procedures to identify ways to protect against similar incidents.

Out of an abundance of caution, the City is providing potentially affected individuals with access to complimentary credit monitoring and identity restoration 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.

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. On May 18, 2021, the City completed its review of the employees' compromised accounts 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 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 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 1-855-763-0063, 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.idheadquarters.com** to activate and take advantage of your identity monitoring services.

*You have until **September 17, 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 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 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 7 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.