



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

July 8, 2024

VIA E-MAIL

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
E-mail: idtheft@oag.state.md.us

Re: Notice of Data Event

To Whom It May Concern:

We represent the City of Philadelphia (the “City”), located at 1515 Arch Street, 17th Floor, Philadelphia, PA 19102, and are writing to notify your office of an event that may affect the security of certain personal information relating to certain Maryland residents. This notice may be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, the City does not waive any rights or defenses regarding the applicability of Maryland law, the applicability of the Maryland data event notification statute, or personal jurisdiction.

Nature of the Data Event

On May 24, 2023, the City became aware of suspicious activity in its email environment. The City 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 gained access to certain City email accounts and certain information contained therein. Also, on August 22, 2023, the City became aware that the at-issue email accounts include accounts that potentially contained protected health information.

The investigation did not determine conclusively whether the unauthorized actor actually accessed or acquired any information. Nonetheless, in an abundance of caution, the City conducted a thorough and in-depth review to determine what information was potentially accessible and to whom such information relates. To ensure compliance with applicable regulations, including the Health Insurance Portability and Accountability Act (“HIPAA”), while the data review was

ongoing, on October 20, 2023, the City also submitted notice to the U.S. Department of Health and Human Services (“HHS”), posted substitute notice on its website, and provided notice to the media in the Philadelphia Inquirer.

Once the City’s review was complete, the City worked to validate the results and locate missing address information for those potentially affected. While this process was ongoing, on May 16, 2024, the City mailed written notice to individuals whose protected health information was potentially impacted (including three Maryland residents), provided supplemental notice to HHS, posted updated notice on its website, and provided updated notice to the media in the Philadelphia Inquirer.

On June 12, 2024, the City finished validating the results of its review and locating missing address information. The personal information related to Maryland residents that was potentially accessible during the event includes the following: name, address, date of birth, Social Security number, driver's license, financial account information, medical information, health insurance information, employer-assigned identification number, and electronic/digital signature.

Notice to Maryland Residents

On July 8, 2024, the City mailed written notice of this event to individuals whose personal information was potentially accessible, including approximately one hundred fifty-one (151) additional Maryland residents. 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 becoming aware of the event, the City moved quickly to investigate and respond to the event, assess the security of its network and email tenant, and identify potentially affected individuals. The City also: notified federal law enforcement; is working to implement additional safeguards and training to its employees; and providing access to credit monitoring services for twelve (12) months to Maryland residents whose personal information was potentially affected by this event, at no cost to these individuals.

Additionally, the City is providing potentially 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 bank, credit card company, or other applicable institution. The City is providing individuals with information on how to place a fraud alert and credit 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.

The City is providing written notice of this event to relevant state regulators, as required, and to the three major credit reporting agencies, Equifax, Experian, and TransUnion.

Office of the Attorney General

July 8, 2024

Page 3

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/aml
Enclosure

EXHIBIT A



CITY OF PHILADELPHIA

LAW DEPARTMENT
One Parkway
1515 Arch Street
Philadelphia, PA 19102-1595

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

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

<<b2b_text_1 (VARIABLE HEADER FIELD)>>

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

The City of Philadelphia (the “City”) is writing to inform you of an event that may impact the security of some of your information. Although we have received no indication of any actual or attempted identity theft or fraud as a result of this event, this notice includes information about the event, our response, and resources available to you to help protect your information from possible misuse, should you feel it is appropriate to do so.

What Happened? On May 24, 2023, the City 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 gained access to certain City email accounts and that certain information contained in those accounts was potentially accessible.

The investigation did not determine conclusively that any information was actually accessed or acquired as a result of the event. Nonetheless, in an abundance of caution, we conducted a thorough and in-depth review to determine what information was potentially accessible and to whom such information relates. Once complete, we also worked to validate the results and locate missing address information for those potentially affected. We recently completed this process, and then worked as quickly as possible to provide notice.

What Information Was Involved? Again, the investigation did not confirm that any information was actually accessed or acquired without authorization. However, the investigation determined that your <<b2b_text_2 (“name,” and impacted data elements)>> were potentially accessible during the event.

What We Are Doing. The confidentiality, privacy, and security of information in our care are among our highest priorities. Upon becoming aware of the event, we moved quickly to investigate and respond to the event, assess the security of our network and email tenant, and notify potentially affected individuals. We are notifying potentially affected individuals, including you, so that you may take further steps to best protect your information, should you feel it is necessary to do so. As an added precaution, we are offering credit monitoring, fraud consultation, and identity theft restoration services through Kroll for <<Monitoring Term Length (Months)>> months, at no cost to you. While the City is covering the cost of these services, you will need to complete the activation process yourself.

What You Can Do. You can learn more about how to help protect yourself against potential information misuse in the enclosed *Steps You Can Take To Help Protect Personal Information*. There, you will find instructions on how to activate in the complimentary credit monitoring, fraud consultation, and identity theft restoration services available to you. We also encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and credits reports for suspicious activity, and to report any suspicious activity promptly to your bank, credit card company, or other applicable institution.

For More Information. We understand that you may have questions about this event that are not addressed in this letter. If you have additional questions, please call the dedicated 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. Please have this letter ready if you call. Again, we take the privacy and security of information in our care very seriously and apologize for any inconvenience or concern this event may cause you.

Sincerely,

Andrew Richman
Chair, Compliance and Legislation Group
City of Philadelphia

STEPS YOU CAN TAKE TO HELP PROTECT PERSONAL INFORMATION

Activate in 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 <<Monitoring Term Length (Months)>> months. 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 <<b2b_text_6(activation deadline)>> to activate your identity monitoring services.

Membership Number: <<Membership Number s_n>>

For more information about Kroll and your Identity Monitoring services, you can visit info.krollmonitoring.com. Additional information describing your services is also included below.



TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES¹

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.

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 a free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. Consumers may also directly contact the three major credit reporting bureaus listed below to request a free copy of their 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 consumers are the victim of identity theft, they are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should consumers wish to place a fraud alert, please contact any 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 a consumer's name without consent. However, consumers should be aware that using a credit freeze to take control over who gets access to the personal and financial information in their credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application they make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, consumers cannot be charged to place or lift a credit freeze on their credit report. To request a credit freeze, individuals may need to provide some or all of the following information:

¹ 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.

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 they are a victim of identity theft.

Should consumers wish to place a credit freeze or fraud alert, 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

Consumers may further educate themselves regarding identity theft, fraud alerts, credit freezes, and the steps they can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or their state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, D.C. 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. Consumers can obtain further information on how to file such a complaint by way of the contact information listed above. Consumers have the right to file a police report if they ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, consumers will likely need to provide some proof that they have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and the relevant 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 Street, NW, 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; 1-410-528-8662 or 1-888-743-0023; and [https://www.marylandattorneygeneral.gov/](http://www.marylandattorneygeneral.gov/).

For New Mexico residents, consumers have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in their credit file has been used against them, the right to know what is in their credit file, the right to ask for their 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 consumers' files is limited; consumers must give consent for credit reports to be provided to employers; consumers may limit "prescreened" offers of credit and insurance based on information in their credit report; and consumers may seek damages from violators. Consumers 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 consumers to review their 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 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.

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, individuals have the right to obtain any police report filed in regard to this event. There are approximately 3 Rhode Island residents that may be impacted by this event.