

Dominic A. Paluzzi
Direct Dial: 248.220.1356
E-mail: dpaluzzi@mcdonaldhopkins.com

January 22, 2024

VIA EMAIL (*Idtheft@oag.state.md.us*)

Office of the Maryland Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202

Re: Upper Merion Township, Pennsylvania - Incident Notification

Dear Sir or Madam:

McDonald Hopkins PLC represents Upper Merion Township (the “Township”). I am writing to provide notification of an incident at the Township that may affect the security of personal information of two (2) Maryland residents. By providing this notice, the Township does not waive any rights or defenses regarding the applicability of Maryland law or personal jurisdiction.

On or about December 27, 2023, the Township discovered that it was the victim of a ransomware incident. The Township immediately engaged this firm and third-party forensic and incident response experts to conduct a thorough investigation of the nature and scope of the incident. The Township recently concluded its initial investigation, which revealed that an unauthorized actor accessed and exfiltrated data from portions of the Township’s network on December 27, 2023.

After an extensive forensic investigation and document review, the Township determined on January 10, 2024 that the impacted files contain personal information of certain individuals, including two (2) Maryland residents. The personal information potentially impacted includes first and last name, driver’s license number, Social Security number, financial account number, and health insurance information.

The Township has no indication that any of the information has been used for identity theft or financial fraud. Nevertheless, out of an abundance of caution, the Township is providing notice to potentially impacted individuals commencing on January 22, 2024 in substantially the same form as the documents attached hereto. The Township is also offering complimentary credit monitoring services to all adult individuals who receive a notification letter, and cyber monitoring services to the parent or guardian of all minors who receive a notification letter. Additionally the Township will advise the affected individuals to remain vigilant in reviewing financial account statements for fraudulent or irregular activity on a regular basis. The Township will further advise the affected individuals about the process for placing a fraud alert and/or security freeze on their credit files and obtaining free credit reports. Finally, the affected individuals are being provided with the contact information for the consumer reporting agencies and the Federal Trade Commission.

January 22, 2024

Page 2

Upper Merion Township is committed to maintaining the privacy of personal information in its possession, and has taken many precautions to safeguard it. The Township continually evaluates and modifies its practices to enhance the security and privacy of the personal information it maintains.

If you have any additional questions, please contact me at (248) 220-1356 or dpaluzzi@mcdonaldhopkins.com.

Very truly yours,



Dominic A. Paluzzi

DAP/jm

Encl.

Exhibit A

Upper Merion Township
c/o Cyberscout
1 Keystone Ave., Unit 700
Cherry Hill, NJ 08003
DB-08390 12-4



Emily Sturz
6914 W Paradise Dr
Peoria, AZ 85345-8741



January 22, 2024

Important Information Please Review Carefully

Dear Emily Sturz:

We are writing with important information regarding a recent data security incident that Upper Merion Township ("Township") experienced which may have impacted your personal information. The privacy and security of the protected personal information entrusted to us is of the utmost importance to the Township. As such, we wanted to provide you with information about the incident, explain the services we are making available to you, and let you know that we continue to take significant measures to protect your information.

While we have no evidence your personal information has been misused in any manner, we are taking appropriate precautionary steps to help alleviate concerns you may have.

What Happened?

The Township detected that some elements of our network had been affected by malware and, as a result, an unauthorized party accessed and/or acquired data from the network on December 27, 2023.

What We Are Doing.

Immediately upon learning of the issue, we commenced a prompt and thorough investigation. As part of our investigation, we have worked closely with external cybersecurity professionals and law enforcement. After an investigation and review of the impacted data, we discovered on January 10, 2024 that the files accessed and/or acquired by the unauthorized actor contained some of your protected personal information.

We want to make you aware of the incident and provide you with steps you can take to protect your information further. Additionally, the Township has reviewed its existing policies and training protocols relating to data protection, while enhancing security measures and monitoring tools to mitigate risk and better prevent similar incidents in the future.

What Information Was Involved?

The data accessed and/or acquired by the unauthorized actor contained some of your protected personal information, including your name, social security number, driver's license number, financial account number, and health insurance information.

What you can do.

To date, we are not aware of any reports of identity fraud or improper use of your information as a direct result of this incident. Nevertheless, out of an abundance of caution and in order to help protect potentially impacted individuals, we are providing you with access to **Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score** services for one year at no

charge. These services provide you with alerts for one year from the date of enrollment when changes occur to your credit file. This notification is sent to you the same day that the change or update takes place with the bureau. Finally, we are providing you with proactive fraud assistance to help with any questions that you might have or in event that you become a victim of fraud. These services will be provided by Cyberscout through Identity Force, a TransUnion company specializing in fraud assistance and remediation services.

How do I enroll for the free services?

To enroll in Credit Monitoring services at no charge, please log on to **<https://secure.identityforce.com/benefit/umt>** and follow the instructions provided. When prompted please provide the following unique code to receive services: **T2J8A3SEBK**

In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter. The enrollment requires an internet connection and e-mail account, and may not be available to minors under the age of 18 years of age. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

For More Information.

Representatives are available for 90 days from the date of this letter, to assist you with questions regarding this incident, between the hours of 8:00 a.m. to 8:00 p.m. Eastern Time, Monday through Friday, excluding holidays. Please call the help line at 1-833-877-8646 and supply the fraud specialist with your unique code listed above.

We are committed to maintaining the privacy of personal information. We continually evaluate and modify our practices and internal controls to enhance the security and privacy of your personal information, including a review of our ongoing third-party vendor relationships.

Sincerely,

A handwritten signature in black ink, appearing to read 'Anthony Hamaday', with a horizontal line extending to the right.

Anthony Hamaday
Township Manager

– OTHER IMPORTANT INFORMATION –

1. Placing a Fraud Alert on Your Credit File.

We recommend that you place an initial one (1) year “fraud alert” on your credit files, at no charge. A fraud alert tells creditors to contact you personally before they open any new accounts. To place a fraud alert, call any one of the three major credit bureaus at the numbers listed below. As soon as one credit bureau confirms your fraud alert, they will notify the others.

If you choose to place a fraud alert on your own, you will need to contact one of the three major credit agencies directly at:

Experian (1-888-397-3742)
P.O. Box 4500
Allen, TX 75013
www.experian.com

Equifax (1-800-525-6285)
P.O. Box 740241
Atlanta, GA 30374
www.equifax.com

TransUnion (1-800-680-7289)
P.O. Box 2000
Chester, PA 19016
www.transunion.com

Also, should you wish to obtain a credit report and monitor it on your own:

- **IMMEDIATELY** obtain free copies of your credit report and monitor them upon receipt for any suspicious activity. You can obtain your free copies by going to the following website: www.annualcreditreport.com or by calling them toll-free at 1-877-322-8228. (Hearing impaired consumers can access their TDD service at 1-877-730-4204.
- **Upon receipt of your credit report**, we recommend that you review it carefully for any suspicious activity.
- Be sure to promptly report any suspicious activity to Upper Merion Township

2. Placing a Security Freeze on Your Credit File.

If you are very concerned about becoming a victim of fraud or identity theft, you may request a “security freeze” be placed on your credit file, at no charge. A security freeze prohibits, with certain specific exceptions, the consumer reporting agencies from releasing your credit report or any information from it without your express authorization. You may place a security freeze on your credit report by contacting all three nationwide credit reporting companies at the numbers below and following the stated directions or by sending a request in writing, by mail, to all three credit reporting companies:

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348-5788
<https://www.equifax.com/personal/credit-report-services/credit-freeze/>
(888)-298-0045

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013
<http://experian.com/freeze>
(888) 397-3742

TransUnion Security Freeze
P.O. Box 160
Woodlyn, PA 19094
<https://www.transunion.com/credit-freeze>
(888) 909-8872

In order to place the security freeze, you’ll need to supply your name, address, date of birth, Social Security number and other personal information. After receiving your freeze request, each credit reporting company will send you a confirmation letter containing a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

If you do place a security freeze *prior* to enrolling in the credit monitoring service as described above, you will need to remove the freeze in order to sign up for the credit monitoring service. After you sign up for the credit monitoring service, you may refreeze your credit file.

3. Obtaining a Free Credit Report.

Under federal law, you are entitled to one free credit report every 12 months from each of the above three major nationwide credit reporting companies. Call **1-877-322-8228** or request your free credit reports online

at **www.annualcreditreport.com**. Once you receive your credit reports, review them for discrepancies. Identify any accounts you did not open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting company.

4. Additional Helpful Resources.

Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Checking your credit report periodically can help you spot problems and address them quickly.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call your local law enforcement agency and file a police report. Be sure to obtain a copy of the police report, as many creditors will want the information it contains to absolve you of the fraudulent debts. You may also file a complaint with the FTC by contacting them on the web at www.ftc.gov/idtheft, by phone at 1-877-IDTHEFT (1-877-438-4338), or by mail at Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580. Your complaint will be added to the FTC's Identity Theft Data Clearinghouse, where it will be accessible to law enforcement for their investigations. In addition, you may obtain information from the FTC about fraud alerts and security freezes.

If your personal information has been used to file a false tax return, to open an account or to attempt to open an account in your name, or to commit fraud or other crimes against you, you may file a police report in the city in which you currently reside.

Dominic A. Paluzzi
Direct Dial: 248.220.1356
E-mail: dpaluzzi@mcdonalddhopkins.com

September 25, 2024

VIA EMAIL (Idtheft@oag.state.md.us)

Office of the Maryland Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202

Re: Upper Merion Township, Pennsylvania - Incident Notification

Dear Sir or Madam:

McDonald Hopkins PLC represents Upper Merion Township (the “Township”). I am writing to supplement notification of an incident at the Township previously provided on January 22, 2024. The Township’s ongoing investigation has identified an additional thirty-nine (39) Maryland residents impacted by this incident. By providing this notice, the Township does not waive any rights or defenses regarding the applicability of Maryland law or personal jurisdiction.

On or about December 27, 2023, the Township discovered that it was the victim of a ransomware incident. The Township immediately engaged this firm and third-party forensic and incident response experts to conduct a thorough investigation of the nature and scope of the incident. The Township recently concluded its initial investigation, which revealed that an unauthorized actor accessed and exfiltrated data from portions of the Township’s network on December 27, 2023.

After an extensive forensic investigation and document review, the Township determined on January 10, 2024 that the impacted files contain personal information of certain individuals, including two (2) Maryland residents. On August 9, 2024, additional individuals were identified as having personal information contained in the files. The personal information potentially impacted includes first and last name, Social Security number, Medicare number, and email address and password.

The Township has no indication that any of the information has been used for identity theft or financial fraud. Nevertheless, out of an abundance of caution, the Township is providing notice to

January 22, 2024

Page 2

potentially impacted individuals commencing on September 25, 2024 in substantially the same form as the documents attached hereto. The Township is also offering complimentary credit monitoring services to all adult individuals who receive a notification letter, and cyber monitoring services to the parent or guardian of all minors who receive a notification letter. Additionally the Township will advise the affected individuals to remain vigilant in reviewing financial account statements for fraudulent or irregular activity on a regular basis. The Township will further advise the affected individuals about the process for placing a fraud alert and/or security freeze on their credit files and obtaining free credit reports. Finally, the affected individuals are being provided with the contact information for the consumer reporting agencies and the Federal Trade Commission.

Upper Merion Township is committed to maintaining the privacy of personal information in its possession, and has taken many precautions to safeguard it. The Township continually evaluates and modifies its practices to enhance the security and privacy of the personal information it maintains.

If you have any additional questions, please contact me at (248) 220-1356 or dpaluzzi@mcdonaldhopkins.com.

Very truly yours,



Dominic A. Paluzzi

DAP/cs

Encl

January 22, 2024

Page 3

Upper Merion Township c/o Cyberscout
PO Box 1286
Dearborn, MI 48120-9998



P



000010102G0400

P

Dear [REDACTED] :

We are writing with important information regarding a recent data security incident that Upper Merion Township ("Township") experienced which may have impacted your personal information. The privacy and security of the protected personal information entrusted to us is of the utmost importance to the Township. As such, we wanted to provide you with information about the incident, explain the services we are making available to you, and let you know that we continue to take significant measures to protect your information.

While we have no evidence your personal information has been misused in any manner, we are taking appropriate precautionary steps to help alleviate concerns you may have.

What Happened?

The Township detected that some elements of our network had been affected by malware and, as a result, an unauthorized party accessed and/or acquired data from the network on December 27, 2023.

What We Are Doing.

Immediately upon learning of the issue, we commenced a prompt and thorough investigation. As part of our investigation, we have worked closely with external cybersecurity professionals and law enforcement. After an investigation and review of the impacted data, we discovered on August 9, 2024 that the files accessed and/or acquired by the unauthorized actor contained some of your protected personal information.

We want to make you aware of the incident and provide you with steps you can take to protect your information further. Additionally, the Township has reviewed its existing policies and training protocols relating to data protection, while enhancing security measures and monitoring tools to mitigate risk and better prevent similar incidents in the future.

What Information Was Involved?

The data accessed and/or acquired by the unauthorized actor contained some of your protected personal information, including your name and [REDACTED].

What you can do.

To date, we are not aware of any reports of identity fraud or improper use of your information as a direct result of this incident. Nevertheless, out of an abundance of caution and in order to help protect potentially impacted individuals, we are providing you with access to **Single Bureau Credit Monitoring** services for [REDACTED] months at no charge. These services provide you with alerts for [REDACTED] from the date of enrollment when changes occur to your credit file. This notification is sent to you the same day that the change or update takes place with the bureau. Finally, we are providing you with proactive fraud assistance to help with any questions that you might have or in event that you become a victim of fraud. These services will be provided by Cyberscout, a TransUnion company specializing in fraud assistance and remediation services.

How do I enroll for the free services?

To enroll in Credit Monitoring services at no charge, please log on to [REDACTED] and follow the instructions provided. When prompted please provide the following unique code to receive services:

In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter. The enrollment requires an internet connection and e-mail account, and may not be available to minors under the age of 18 years of age. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

For More Information.

Representatives are available for 90 days from the date of this letter, to assist you with questions regarding this incident, between the hours of 8:00 a.m. to 8:00 p.m. Eastern Time, Monday through Friday, excluding holidays. Please call the help line at [REDACTED] and supply the fraud specialist with your unique code listed above.

We are committed to maintaining the privacy of personal information. We continually evaluate and modify our practices and internal controls to enhance the security and privacy of your personal information, including a review of our ongoing third-party vendor relationships.

Sincerely,



Anthony Hamaday
Township Manager



- OTHER IMPORTANT INFORMATION -

1. Placing a Fraud Alert on Your Credit File.

We recommend that you place an initial one (1) year “fraud alert” on your credit files, at no charge. A fraud alert tells creditors to contact you personally before they open any new accounts. To place a fraud alert, call any one of the three major credit bureaus at the numbers listed below. As soon as one credit bureau confirms your fraud alert, they will notify the others.

If you choose to place a fraud alert on your own, you will need to contact one of the three major credit agencies directly at:

Experian (1-888-397-3742)

Equifax (1-800-525-6285)

TransUnion (1-800-680-7289)

P.O. Box 4500

P.O. Box 740241

P.O. Box 2000

Allen, TX 75013 Atlanta, GA 30374 Chester, PA 19016 www.experian.com www.equifax.com
www.transunion.com

Also, should you wish to obtain a credit report and monitor it on your own:

- **IMMEDIATELY** obtain free copies of your credit report and monitor them upon receipt for any suspicious activity. You can obtain your free copies by going to the following website: www.annualcreditreport.com or by calling them toll-free at 1-877-322-8228. (Hearing impaired consumers can access their TDD service at 1-877-730-4204.
- **Upon receipt of your credit report**, we recommend that you review it carefully for any suspicious activity.
- Be sure to promptly report any suspicious activity to Upper Merion Township

2. Placing a Security Freeze on Your Credit File.

If you are very concerned about becoming a victim of fraud or identity theft, you may request a “security freeze” be placed on your credit file, at no charge. A security freeze prohibits, with certain specific exceptions, the consumer reporting agencies from releasing your credit report or any information from it without your express authorization. You may place a security freeze on your credit report by contacting all three nationwide credit reporting companies at the numbers below and following the stated directions or by sending a request in writing, by mail, to all three credit reporting companies:

Equifax Security Freeze

P.O. Box 105788

Atlanta, GA 30348-5788

<https://www.equifax.com/personal/credit-report-services/credit-freeze/>

(888)-298-0045

Experian Security Freeze

P.O. Box 9554

Allen, TX 75013

<http://experian.com/freeze>

(888) 397-3742

TransUnion Security Freeze

P.O. Box 160

Woodlyn, PA 19094

<https://www.transunion.com/credit-freeze>

(888) 909-8872

In order to place the security freeze, you'll need to supply your name, address, date of birth, Social Security number and other personal information. After receiving your freeze request, each credit reporting company will send you a confirmation letter containing a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

If you do place a security freeze *prior* to enrolling in the credit monitoring service as described above, you will need to remove the freeze in order to sign up for the credit monitoring service. After you sign up for the credit monitoring service, you may refreeze your credit file.

3. Obtaining a Free Credit Report.

Under federal law, you are entitled to one free credit report every 12 months from each of the above three major nationwide credit reporting companies. Call **1-877-322-8228** or request your free credit reports online at **www.annualcreditreport.com**. Once you receive your credit reports, review them for discrepancies. Identify any accounts you did not open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting company.

4. Additional Helpful Resources.

Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Checking your credit report periodically can help you spot problems and address them quickly.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call your local law enforcement agency and file a police report. Be sure to obtain a copy of the police report, as many creditors will want the information it contains to absolve you of the fraudulent debts. You may also file a complaint with the FTC by contacting them on the web at www.ftc.gov/idtheft, by phone at 1-877-IDTHEFT (1-877-438-4338), or by mail at Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580. Your complaint will be added to the FTC's Identity Theft Data Clearinghouse, where it will be accessible to law enforcement for their investigations. In addition, you may obtain information from the FTC about fraud alerts and security freezes.

If your personal information has been used to file a false tax return, to open an account or to attempt to open an account in your name, or to commit fraud or other crimes against you, you may file a police report in the city in which you currently reside.

Iowa Residents: You may contact law enforcement or the Iowa Attorney General's Office to report suspected incidents of identity Theft: Office of the Attorney General of Iowa, Consumer Protection Division, Hoover State Office Building, 1305 East Walnut Street, Des Moines, IA 50319, www.iowaattorneygeneral.gov, Telephone: 515-281-5164.

Maryland Residents: You may obtain information about avoiding identity theft from the Maryland Attorney General's Office: Office of the Attorney General of Maryland, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, <https://www.marylandattorneygeneral.gov/>, Telephone: 888-743-0023.

New York Residents: You may obtain information about preventing identity theft from the New York Attorney General's Office: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; <https://ag.ny.gov/consumer-frauds-bureau/identity-theft>; Telephone: 800-771-7755.

North Carolina Residents: You may obtain information about preventing identity theft from the North Carolina Attorney General's Office: Office of the Attorney General of North Carolina, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov/, Telephone: 877-566-7226 (Toll-free within North Carolina), 919-716-6000.

Oregon Residents: You may obtain information about preventing identity theft from the Oregon Attorney General's Office: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 877-877-9392.

Washington D.C. Residents: You may obtain information about preventing identity theft from the Office of the Attorney General for the District of Columbia, 400 6th Street NW, Washington D.C. 20001, <https://oag.dc.gov/consumer-protection>, Telephone: 202-442-9828.