

Spencer S. Pollock, CIPP/US, CIPM
Direct Dial: 1.410.456.2741
Cell: 1.410.917.5189
Email: spollock@mcdonaldhopkins.com

May 30, 2023

VIA EMAIL: Idtheft@oag.state.md.us

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

Re: Wickersham Construction & Engineering, Inc. – Incident Notification

Dear Mr. Brown:

McDonald Hopkins PLC represents Wickersham Construction & Engineering, Inc. (“Wickersham”) located at 777 E Ross St, Lancaster, PA 17602. I am writing to provide notification of an incident on behalf of Wickersham that may affect the security of personal information of three (3) Maryland residents. By providing this notice, Wickersham does not waive any rights or defenses regarding the applicability of Maryland law or personal jurisdiction.

Wickersham detected unauthorized access to certain systems on its network as a result of a cybersecurity incident. The incident resulted in the unauthorized access and/or acquisition of certain files from portions of the network. Upon detecting the incident, Wickersham commenced an immediate and thorough investigation and contained the network. As part of our investigation, Wickersham engaged leading cybersecurity professionals to identify the extent of the activity and what, if any, individual personal information may have been accessed and/or acquired by the unauthorized party. The information involved includes name and social security number.

After a thorough and detailed forensic investigation and comprehensive manual document review, Wickersham determined on April 27, 2023, that an unauthorized party may have accessed or acquired individual personal information between September 16, 2022 and September 19, 2022. On May 23, 2023, Wickersham found the names and most recent contact information of the Maryland residents involved.

Wickersham provided the affected residents with written notification of this incident to individuals commencing on May 30, 2023, in substantially the same form as the letter attached hereto.

May 30, 2023

Page 2

Wickersham is not aware of any reports of identity fraud or improper use of personal information as a direct result of this incident. However, out of an abundance of caution, Wickersham wanted to inform your Office (and the affected residents) of the incident. Notified individuals have been provided with best practices to protect their information, including but not limited to complimentary credit monitoring services.

At Wickersham, protecting the privacy of personal information is a top priority. Wickersham is committed to maintaining the privacy of personal information in its possession and has taken precautions to safeguard it. Wickersham 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 (410) 456-2741 or spollock@mcdonaldhopkins.com.

Very truly yours,



Spencer S. Pollock

Encl.

Wickersham Construction & Engineering, Inc.
c/o Cyberscout
1 Keystone Ave., Unit 700
Cherry Hill, NJ 08003
DB07444



May 30, 2023

***IMPORTANT INFORMATION
PLEASE REVIEW CAREFULLY***

Dear [REDACTED]:

We are writing with important information regarding a data security incident that affected our organization. The privacy and security of the personal information we maintain is of the utmost importance to Wickersham Construction & Engineering, Inc. ("Wickersham"). 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 personal information.

What Happened?

Wickersham detected unauthorized access to certain systems on its network as a result of a cybersecurity incident. The incident resulted in the unauthorized access and/or acquisition of certain files from portions of the network.

What We Are Doing

Upon detecting the incident, Wickersham commenced an immediate and thorough investigation and contained the network. As part of our investigation, Wickersham engaged leading cybersecurity professionals to identify the extent of the activity and what, if any, individual personal information may have been accessed and/or acquired by the unauthorized party. After a thorough and detailed forensic investigation and comprehensive manual document review of the files involved in the incident, on April 27, 2023, Wickersham determined that your personal information may have been accessed or acquired by an unauthorized party between September 16, 2022 and September 19, 2022.

What Information Was Involved

The data potentially involved included your full name along with Date Of Birth, Email, Home Phone, Social Security Number.

What You Can Do

To protect you from the potential misuse of your information, we are providing you access to Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score services at no charge. These services provide you with alerts for 12 months 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. This service is completely free to you, and enrolling in this program will not hurt your credit score. For

more information on identity theft prevention, including instructions on how to activate your complimentary 12 months membership, please see the additional information provided in this letter.

This letter also provides other precautionary measures you can take to protect your information from potential misuse, including placing a fraud alert and/or security freeze on your credit files, and/or obtaining a free credit report. Additionally, you should always remain vigilant in reviewing your financial account statements and credit reports on a regular basis for fraudulent or irregular activity.

Please accept our apology that this incident occurred. We are committed to maintaining the privacy of your information and have taken many precautions to help safeguard it. We continually evaluate and modify our practices to enhance the security and privacy of the personal information in our possession, and have taken steps to further protect unauthorized access to individual records.

For More Information

If you have any further questions regarding this incident, please call our dedicated and confidential toll-free response line that we have established to respond to questions surrounding the incident at [REDACTED]. This response line is staffed with professionals familiar with this incident and knowledgeable on what you can do to protect against misuse of your information. The response line is available Monday through Friday, from 8:00 a.m. to 8:00 p.m. Eastern Time, excluding holidays.

Sincerely,

Wickersham Construction & Engineering, Inc

OTHER IMPORTANT INFORMATION

1. Enrolling in Complimentary 12 months Credit Monitoring.

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: [REDACTED]. 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.

2. Placing a Fraud Alert on Your Credit File.

We recommend that you place an initial one-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.

Equifax

P.O. Box 105069
Atlanta, GA 30348
www.equifax.com
1-800-525-6285

Experian

P.O. Box 2002
Allen, TX 75013
www.experian.com
1-888-397-3742

TransUnion LLC

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

3. 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
<https://www.freeze.equifax.com>
1-800-349-9960

Experian Security Freeze

P.O. Box 9554
Allen, TX 75013
<http://experian.com/freeze>
1-888-397-3742

TransUnion Security Freeze

P.O. Box 2000
Chester, PA 19016
<http://www.transunion.com/securityfreeze>
1-888-909-8872

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 any credit monitoring service, 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.

4. 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.

5. 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.

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, www.oag.state.md.us/Consumer, 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.