

Heather Shumaker
Direct Dial: 248.402.4066
E-mail: hshumaker@mcdonaldhopkins.com

April 9, 2024

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

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

Re: Smith Sovik Kendrick & Sugnet P.C. – Incident Notification

Dear Mr. Brown:

McDonald Hopkins PLC represents Smith Sovik Kendrick & Sugnet P.C. (“Smith Sovik”) located at 250 South Clinton Street, Suite 600, Syracuse, New York 13202. I am writing to provide notification of an incident on behalf of Smith Sovik that may affect the security of personal information of one (1) Maryland resident(s). By providing this notice, Smith Sovik does not waive any rights or defenses regarding the applicability of Maryland law or personal jurisdiction.

On or around May 28, 2023, Smith Sovik detected that a network security event involving unauthorized access to its network. Upon detecting the incident, Smith Sovik commenced an immediate and thorough investigation. As part of the investigation, Smith Sovik worked to identify what personal information, if any, might have been present in the accessed systems.

After a thorough and detailed forensic investigation, Smith Sovik determined on March 25, 2024, that resulting from the unauthorized access that between May 4, 2023 and May 28, 2023, an unauthorized party accessed and/or acquired certain files pertaining to a limited number of individuals. This information included full name and driver’s license number.

Smith Sovik 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, Smith Sovik wanted to inform your Office (and the affected resident(s)) of the incident. Affected residents will be notified of the incident starting on April 9, 2024. Notified individuals will be provided with best practices to protect their information, including but not limited to complimentary credit monitoring services. Smith Sovik will advise the affected resident to

April 9, 2024

Page 2

always remain vigilant in reviewing financial account statements for fraudulent or irregular activity on a regular basis. Smith Sovik will advise the affected resident about the process for placing a fraud alert and/or security freeze on their credit files and obtaining free credit reports. The affected resident is also being provided with the contact information for the consumer reporting agencies and the Federal Trade Commission and the Maryland Attorney General.

At Smith Sovik, protecting the privacy of personal information is a top priority. Smith Sovik is committed to maintaining the privacy of personal information in its possession and has taken precautions to safeguard it. Smith Sovik continually evaluates and modifies its practices to enhance the security and privacy of the personal information it maintains.

Should you have any questions regarding this notification, please contact me at (248) 402-4066 or hshumaker@mcdonaldhopkins.com.

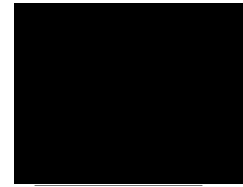
Very truly yours,

A handwritten signature in black ink, appearing to read 'H. Shumaker', with a long horizontal flourish extending to the right.

Heather Shumaker

Enrollment Code: 

To Enroll, Scan the QR Code Below:



Or Visit:



IMPORTANT INFORMATION PLEASE REVIEW CAREFULLY



Dear :

The privacy and security of the personal information we maintain is of the utmost importance to Smith Sovik Kendrick & Sugnet P.C. ("Smith Sovik"). We are writing with important information regarding a recent data security incident that involved some of your information. We want to provide you with information about the incident, inform you about the services we are providing to you, and let you know that we continue to take significant measures to protect your information.

What Happened?

On May 28, 2023, Smith Sovik detected that an unauthorized party obtained access to a computer on our network.

What We Are Doing.

Upon learning of this issue, we contained the threat by disabling all unauthorized access to our network and immediately commenced a prompt and thorough investigation. As part of our investigation, we have been working very closely with external cybersecurity professionals experienced in handling these types of incidents. Through the investigation into the incident, Smith Sovik determined on March 25, 2024, that between May 4, 2023 and May 28, 2023, the unauthorized party may have removed certain files and folders from the network and that those files may contain personal information.

What Information Was Involved?

The impacted files contain some of your personal information, specifically your name and, .

What You Can Do.

We have no evidence that any of your information has been misused. Nevertheless, out of an abundance of caution, we want to make you aware of the incident. To protect you from potential misuse of your information, we are offering a complimentary  membership of identity theft protection services through IDX, A ZeroFox Company. IDX identity protection services include:  of credit and CyberScan monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed id theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised.

This letter also provides precautionary measures you can take to protect your personal information, including placing a Fraud Alert and Security Freeze on your credit files, and obtaining a free credit report. Additionally, you should always remain vigilant in reviewing your financial account statements and credit reports for fraudulent or irregular activity on a regular basis.

For More Information.

Please accept our apologies that this incident occurred. We remain fully committed to maintaining the privacy of personal information in our possession and have taken many precautions to safeguard it. We continually evaluate and modify our practices to enhance the security and privacy of your personal information.

If you have any further questions regarding this incident, please call our dedicated and confidential toll-free response line that we have set up to respond to questions 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, 9:00am – 9:00pm Eastern time.

Sincerely,

Smith Sovik Kendrick & Sugnet P.C.
250 South Clinton Street, Suite 600
Syracuse, New York 13202

– OTHER IMPORTANT INFORMATION –

1. Enrolling in Complimentary [REDACTED] of Credit Monitoring.

1. Website and Enrollment. Scan the QR image or go to [REDACTED] and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter. The deadline to enroll is July 8, 2024.

2. Activate the credit monitoring provided as part of your IDX identity protection membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.

3. Telephone. Contact IDX at [REDACTED] to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

2. Placing a Fraud Alert on Your Credit File.

Whether or not you choose to use the complimentary [REDACTED] of credit monitoring services, 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.

Equifax

P.O. Box 105788
Atlanta, GA 30348

<https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/>
(800) 525-6285

Experian

P.O. Box 9554
Allen, TX 75013

<https://www.experian.com/fraud/center.html>
(888) 397-3742

TransUnion LLC

P.O. Box 6790
Fullerton, CA 92834-6790

<https://www.transunion.com/fraud-alerts>
(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.equifax.com/personal/credit-report-services/credit-freeze/>
(800) 349-9960

Experian Security Freeze

P.O. Box 9554
Allen, TX 75013

<http://experian.com/freeze>
(888) 397-3742

TransUnion Security Freeze

P.O. Box 2000
Chester, PA 19016

<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.

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.