

Colin M. Battersby
Direct Dial: (248) 593-2952
E-mail: cbattersby@mcdonaldhopkins.com

February 23, 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: Somerville & Wilkinson, Ltd. – Incident Notification

Dear Sir or Madam:

McDonald Hopkins PLC represents Somerville & Wilkinson, Ltd (“Somerville”). I am writing to provide notification of an incident at Somerville that may affect the security of personal information of four (4) Maryland residents. By providing this notice, Somerville does not waive any rights or defenses regarding the applicability of Maryland law or personal jurisdiction.

Somerville recently learned that an unauthorized individual gained access to its title assistant’s email account. Upon learning of this issue, Somerville contained and secured the threat and commenced a prompt and thorough investigation. As part of the investigation, Somerville has been working very closely with external cybersecurity professionals experienced in handling these types of incidents.

Following a forensics investigation and internal review of the impacted emails, Somerville discovered on January 25, 2024 that files containing personal information were accessed and potentially acquired by an unauthorized party between October 12, 2023 and November 6, 2023. The potentially impacted information includes Social Security number, financial account number, and financial institution name.

Somerville has no indication that any of the information has been used for identity theft or financial fraud. Nevertheless, out of an abundance of caution, Somerville is providing notice to the affected residents commencing on February 23, 2024 in substantially the same form as the document attached hereto. Somerville is also offering complimentary credit monitoring to the impacted residents. Additionally Somerville will advise the affected residents to always remain vigilant in reviewing financial account statements for fraudulent or irregular activity on a regular basis. Somerville will further advise the affected residents about the process for placing a fraud alert and/or security freeze on their credit files and obtaining free credit reports. The affected residents is also being provided with the contact information for the consumer reporting agencies and the Federal Trade Commission.

At Somerville, protecting the privacy of personal information is a top priority. Somerville is committed to maintaining the privacy of personal information in its possession and has taken many precautions to safeguard it. Somerville 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) 593-2952 or cbattersby@mcdonaldhopkins.com.

Very truly yours,

A handwritten signature in blue ink, appearing to read 'Colin M. Battersby', with a large, stylized initial 'C'.

Colin M. Battersby

Encl.

SOMERVILLE & WILKINSON, LTD.

ATTORNEY AT LAW

RICHARD K. WILKINSON
[REDACTED]

INTEGRITY TITLE COMPANY, LLC
EMILY K. RINER, VA LICENSE NO. [REDACTED]
[REDACTED]

243 E CHURCH STREET
POST OFFICE BOX 629
ORANGE, VIRGINIA 22960
TELEPHONE [REDACTED]
FACSIMILE [REDACTED]

ATWELL W. SOMERVILLE
[REDACTED]

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

[REDACTED]

[REDACTED]

Dear [REDACTED]:

The privacy and security of the personal information we maintain is of the utmost importance to the Somerville & Wilkinson, Ltd (“Somerville”). We are writing with important information regarding a security incident that may have involved your personal information. As such, we want to provide you with information about the incident, tell 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?

Somerville recently learned that an unauthorized individual gained access to our title assistant’s email account.

What We Are Doing

Upon learning of this issue, we contained and secured the threat and 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.

What Information Was Involved?

Following a forensics investigation and internal review of the impacted emails, we discovered on January 25, 2024 that files containing your full name and [REDACTED] were accessed and potentially acquired by an unauthorized party between October 12, 2023 and November 6, 2023.

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 help protect your information, we are offering a complimentary 12-month membership of Experian IdentityWorksSM. This product helps detect possible misuse of your personal information and provides you with identity protection services focused on immediate identification and resolution of identity theft. IdentityWorks is completely free to you and enrolling in this program will not hurt your credit score. For more information on identity theft prevention and IdentityWorks, including instructions on how to activate your complimentary one-year membership, please see the additional information provided in this letter.

This letter also provides other 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. If your bank account information was impacted, we recommend that you contact your financial institution to

inquire about steps to take to protect your account, including whether you should close your account or obtain a new account number. 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 are committed to maintain the privacy of personal information in our possession and have taken many precautions to safeguard it. We continually evaluate and modify our practices and internal controls to enhance the security and privacy of your personal information, including updating passwords and enhancing email access protocols. If you have any further questions regarding this incident, please contact [REDACTED]

Sincerely,

Somerville & Wilkinson, Ltd

– OTHER IMPORTANT INFORMATION –

1. **Enrolling in Complimentary 12-Month Credit Monitoring.**

Activate IdentityWorks Credit 3B Now in Three Easy Steps

1. ENROLL by: [REDACTED] (Your code will not work after this date.)
2. VISIT the **Experian IdentityWorks website** to enroll: [REDACTED]
3. PROVIDE the **Activation Code**: [REDACTED]

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 877-288-8057. Be prepared to provide engagement number [REDACTED] as proof of eligibility for the identity restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 12-MONTH EXPERIAN IDENTITYWORKS CREDIT 3B MEMBERSHIP:

A credit card is **not** required for enrollment in Experian IdentityWorks Credit 3B.

You can contact Experian **immediately without needing to enroll in the product** regarding any fraud issues. Identity Restoration specialists are available to help you address credit and non-credit related fraud.

Once you enroll in Experian IdentityWorks, you will have access to the following additional features:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Actively monitors Experian, Equifax and Transunion files for indicators of fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **\$1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

**Activate your membership today at [REDACTED]
or call [REDACTED] to register with the activation code above.**

What you can do to protect your information: There are additional actions you can consider taking to reduce the chances of identity theft or fraud on your account(s). Please refer to www.ExperianIDWorks.com/restoration for this information. If you have any questions about IdentityWorks, need help understanding something on your credit report or suspect that an item on your credit report may be fraudulent, please contact Experian's customer care team at 877-288-8057.

* Offline members will be eligible to call for additional reports quarterly after enrolling.

** Identity theft insurance is underwritten by insurance company subsidiaries or affiliates of American International Group, Inc. (AIG). The description herein is a summary and intended for informational purposes only and does not include all terms, conditions and exclusions of the policies described. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

2. Placing a Fraud Alert.

You can 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 30348-5069
<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

Fraud Victim Assistance
Department
P.O. Box 2000
Chester, PA 19016-2000
<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
(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.

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 this notice letter states that your financial account information and/or credit or debit card information was impacted, we recommend that you contact your financial institution to inquire about steps to take to protect your account, including whether you should close your account or obtain a new account number.

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, <https://www.marylandattorneygeneral.gov/>, Telephone: 888-743-0023.

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.