

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

RECEIVED
SEP 28 2020
CONSUMER PROTECTION

September 21, 2020

VIA U.S. MAIL

Attorney General Gordon MacDonald
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

Re: Brody Wilkson PC – Incident Notification

Dear Attorney General MacDonald:

McDonald Hopkins PLC represents Brody Wilkinson PC. I am writing to provide notification of an incident at Brody Wilkinson PC that may affect the security of personal information of approximately four (4) New Hampshire residents. Brody Wilkinson PC's investigation is ongoing, and this notification will be supplemented with any new or significant facts or findings subsequent to this submission, if any. By providing this notice, Brody Wilkinson PC does not waive any rights or defenses regarding the applicability of New Hampshire law or personal jurisdiction.

An unauthorized individual obtained access to a limited number of Brody Wilkinson PC employee email accounts between January 29, 2020 and February 6, 2020. Upon learning of the potential issue, Brody Wilkinson PC immediately launched an investigation in consultation with outside cybersecurity professionals who regularly investigate and analyze these types of situations to determine the extent of any compromise of the email accounts and the security of the emails and attachments contained within them. Brody Wilkinson PC devoted considerable time and effort to determine what information was contained in the affected email accounts. Based on its comprehensive investigation and document review, which concluded on September 2, 2020, Brody Wilkinson PC discovered that the compromised email accounts contained a limited amount of personal information, including the affected residents' full names and Social Security numbers.

To date, Brody Wilkinson PC is not aware of any reports of identity fraud or improper use of the affected residents' or anyone else's information as a result of this incident. Nevertheless, out of an abundance of caution, Brody Wilkinson PC wanted to inform you (and the affected residents) of the incident and to explain the steps that it is taking to help safeguard the affected residents against identity fraud. Brody Wilkinson PC is providing the affected residents with written notification of this incident commencing on or about September 22, 2020 in substantially the same form as the letter attached hereto. Brody Wilkinson PC is offering the affected residents

Attorney General Gordon MacDonald
Office of the Attorney General
September 21, 2020
Page 2

complimentary one-year memberships with a credit monitoring service. Brody Wilkinson PC is advising the affected residents about the process for placing fraud alerts and/or security freezes on their credit files and obtaining free credit reports. The affected residents are also being provided with the contact information for the consumer reporting agencies and the Federal Trade Commission.

At Brody Wilkinson PC, protecting the privacy of personal information is a top priority. Brody Wilkinson PC is committed to maintaining the privacy of personal information in its possession. Brody Wilkinson PC has implemented additional safeguards designed to prevent a recurrence of any similar incident. Brody Wilkinson PC continually evaluates and modifies its practices and internal controls to enhance the security and privacy of personal information with the advice of technology security professionals.

Should you have any questions concerning this notification, please contact me at (248) 593-2952 or cbattersby@mcdonaldhopkins.com. Thank you for your cooperation.

Very truly yours,



Colin M. Battersby

Encl.

Brody Wilkinson PC

Mail Handling Services
777 E Park Dr
Harrisburg, PA 17111



**IMPORTANT INFORMATION
PLEASE REVIEW CAREFULLY**

September 22, 2020

Dear [REDACTED]:

We are writing with information regarding a security incident that occurred earlier this year. The privacy and security of the personal information we maintain is of the utmost importance to Brody Wilkinson PC. We wanted to provide you with some details 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?

An unauthorized individual likely operating outside of the United States obtained access to a limited number of Brody Wilkinson PC employee email accounts between January 29, 2020 and February 6, 2020.

What We Are Doing.

Upon learning of the potential issue, we immediately launched an investigation in consultation with outside cybersecurity professionals who regularly investigate and analyze these types of situations to determine the extent of any compromise of the email accounts and the security of the emails and attachments contained within them. We devoted considerable time and effort to determine what information was contained in the affected email accounts.

What Information Was Involved?

Based on our comprehensive investigation and document review, which concluded on September 2, 2020, we discovered that the compromised email account(s) contained your full name, Social Security number, and driver's license number.

What You Can Do.

To date, we are not aware of any reports of identity fraud or improper use of any of your or anyone else's information as a result of this incident. Additionally, we believe the purpose of the unauthorized access was to obtain immediate financial gain through attempted wire fraud, and not the acquisition of sensitive data for any other wrongful purpose. Nevertheless, out of an abundance of caution, we wanted to make you aware of the incident, explain the services we are making available to help safeguard you against identity fraud, and suggest steps that you should take as well. To protect you from potential misuse of your information, we are offering a complimentary one-year membership of Experian IdentityWorksSM Credit 3B. 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 Credit 3B 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 Credit 3B, 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/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 for fraudulent or irregular activity on a regular basis.

For More Information.

We regret any inconvenience this incident has caused you. We are committed to maintaining the privacy of personal information in our possession. We have implemented additional safeguards designed to prevent a recurrence of any similar incident. We continually evaluate and modify our practices and internal controls to enhance the security and privacy of your personal information with the advice of technology security professionals.

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, 8am to 5pm Eastern Time.

Sincerely,

Brody Wilkinson PC

– 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 [REDACTED]. 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.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **Up to \$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 [REDACTED] 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 [REDACTED].

* 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 on Your Credit File.

Whether or not you choose to use the complimentary 12 month credit monitoring services, 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. Consider 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 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 municipality in which you currently reside.

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.