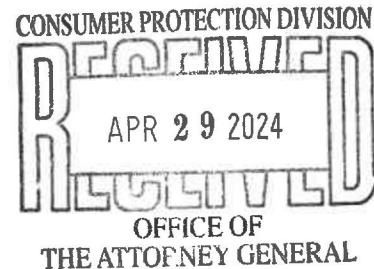


Colin Battersby
Direct Dial: 248.593.2952
E-mail: cbattersby@mcdonaldhopkins.com

April 23, 2024

VIA MAIL

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



Re: Conte Wealth Advisors – Incident Notification

Dear Sir or Madam:

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

On October 23, 2023, Conte learned that an unauthorized individual may have obtained access to a Conte email account. Upon learning of this issue, Conte immediately commenced a prompt and thorough investigation working very closely with external cybersecurity professionals experienced in handling these types of incidents to determine whether there was any unauthorized access to protected information. After an extensive forensic investigation and document review, Conte learned on March 22, 2024, that a limited amount of personal information contained in the impacted email account may have been accessed by the unauthorized individual. The information potentially accessed includes full name, Social Security number, driver’s license/Government ID number, and bank/financial account and routing number. The type of impacted information varies by individual and not all elements were necessarily impacted.

Conte has no indication that any of the information has been used for identity theft or financial fraud. Nevertheless, out of an abundance of caution, Conte is providing notice to the affected residents commencing on April 24, 2024, in substantially the same form as the document attached hereto. Conte is also offering complimentary credit monitoring to the impacted residents whose Social Security number were potentially impacted. Additionally, Conte will advise the affected residents to always remain vigilant in reviewing financial account statements for fraudulent or irregular activity on a regular basis. Conte 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 are also being provided with the contact information for the consumer reporting agencies and the Federal Trade Commission and the Maryland Attorney General

At Conte, protecting the privacy of personal information we maintain is a top priority. Conte is committed to maintaining the privacy of personal information in its possession and has

taken many precautions to safeguard it. Conte 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 at cbattersby@mcdonaldhopkins.com

Very truly yours,

A handwritten signature in blue ink, appearing to read 'Colin Battersby', with a large, sweeping loop at the end.

Colin Battersby

Encl.



Dear [REDACTED]

The privacy and security of the personal information we maintain is of the utmost importance to Conte Wealth Advisors ("Conte"). We are writing with important information regarding a recent data security incident that potentially involved some of your personal information. As such, we want 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.

What Happened?

On or around October 23, 2023, Conte learned that an unauthorized individual obtained access to an employee email account that resulted in the potential exposure of your personal information.

What We Are Doing.

Upon learning of this issue, we 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. After an extensive forensic investigation, we learned on March 22, 2024 that certain emails containing personal information may have been accessed by the unauthorized party.

We currently have no evidence indicating that any personal information has been used for identity theft or financial fraud as a result of the incident. However, out of an abundance of caution, we wanted to notify you of the incident and provide you with information on steps you can take to help protect your information.

What Information Was Involved?

The compromised email account contained your full name, and your [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, to protect you from potential misuse of your information, we are offering a complimentary [REDACTED] month membership with 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. Experian 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 [REDACTED] month 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. To the extent it is helpful, we have also provided information on protecting your medical information on the following pages.

For More Information.

Please accept our apologies that this incident occurred. We are 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 and internal controls 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 [REDACTED] EST.

Sincerely,

Conte Wealth Advisors

– OTHER IMPORTANT INFORMATION –

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

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 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] 7 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.

2. Placing a Fraud Alert on Your Credit File.

Whether or not you choose to use the complimentary 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 30348-5069
<https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/>
(800) 685-1111

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. 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 30348-5788
<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 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.

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.

6. **Protecting Your Medical Information.**

The following practices can provide additional safeguards to protect against medical identity theft.

- Only share your health insurance cards with your health care providers and other family members who are covered under your insurance plan or who help you with your medical care.
- Review your “explanation of benefits statement” which you receive from your health insurance company. Follow up with your insurance company or care provider for any items you do not recognize. If necessary, contact the care provider on the explanation of benefits statement and ask for copies of medical records from the date of the potential access (noted above) to current date.
- Ask your insurance company for a current year-to-date report of all services paid for you as a beneficiary. Follow up with your insurance company or the care provider for any items you do not recognize.

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.

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.