

RECEIVED

JUN 08 2026

McDonald Hopkins PLC  
1820 Lancaster Street  
Suite 200  
Baltimore, MD 21231

CONSUMER PROTECTION

**Razvan E. Miutescu**  
Direct Dial: (410) 926-0136  
E-mail: [rmiutescu@mcdonaldhopkins.com](mailto:rmiutescu@mcdonaldhopkins.com)

June 2, 2026

**VIA U.S. MAIL**

John M. Formella  
Office of the Attorney General  
Consumer Protection Bureau  
33 Capitol Street  
Concord, NH 03301

**Re: DBR & CO – Incident Notification**

To Whom It May Concern:

McDonald Hopkins PLC represents D.B. Root & Company, LLC (“**DBR & CO**”). I am writing to provide notification of an incident at DBR & CO that may affect the security of personal information of approximately seven (7) residents. By providing this notice, DBR & CO does not waive any rights or defenses regarding the applicability of New Hampshire law or personal jurisdiction.

On or about November 12, 2025, DBR & CO experienced unauthorized access to its email systems (“the Incident”). Upon learning of this, DBR & CO commenced an investigation with external cybersecurity professionals experienced in handling these types of situations to help determine whether any personal sensitive data was compromised as a result of the Incident. After a forensic investigation and manual document review, DBR & CO discovered on May 13, 2026, that that some of the emails that were potentially removed from the system by an unauthorized third-party actor on or around November 11, 2025, contained personal information. The information impacted included individuals’ full name, social security number and account information. Upon this discovery, DBR & CO proceeded to notify the impacted residents.

DBR & CO 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. DBR & CO is providing the affected residents with written notification of this incident commencing on May 27, 2026, in substantially the same form as the letter attached hereto. DBR & CO is offering the residents with Social Security numbers impacted a complimentary membership to a credit monitoring service. DBR & CO has also provided the affected residents with contact information for the FTC, and the major credit reporting agencies.

At DBR & CO, protecting the privacy of personal information is a priority. DBR & CO is committed to maintaining the privacy of personal information in its possession and has taken

Page 2

many precautions to safeguard it. DBR & CO 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) 926-0136 or [rmiutescu@mcdonaldhopkins.com](mailto:rmiutescu@mcdonaldhopkins.com).

Very truly yours,

A handwritten signature in blue ink, appearing to read "Razvan E. Miutescu". The signature is fluid and cursive, with a large initial "R" and "M".

Razvan E. Miutescu

Encl.

<<Return to Kroll>>  
<<Return Address>>  
<<City, State ZIP>>



<<FIRST\_NAME>> <<MIDDLE\_NAME>> <<LAST\_NAME>> <<SUFFIX>>  
<<ADDRESS\_1>>  
<<ADDRESS\_2>>  
<<CITY>>, <<STATE\_PROVINCE>> <<POSTAL\_CODE>>  
<<COUNTRY>>



<<Date>> (Format: Month Day, Year)

<<b2b\_text\_1 (VARIABLE HEADER)>>

Dear <<First\_Name>> <<Last\_Name>>:

The privacy and security of the personal information DBR & CO maintains is of the utmost importance. As such, we want to provide you with information about a recent data security incident, tell you about the services that we are providing to you, and let you know that we continue to take significant measures to protect your information.

### **What Happened?**

On or about November 11, 2025, we learned that an unauthorized individual may have gained access to DBR & CO's network.

### **What We Are Doing**

Upon learning of this, we immediately secured our network and commenced a prompt and thorough investigation. As part of our investigation, we have been working closely with external cybersecurity professionals experienced in handling these types of incidents. After an extensive forensic investigation and comprehensive document review, on April 9, 2026, we determined that between November 11-12, 2025, a limited amount of your personal information may have been subject to unauthorized acquisition.

### **What Information Was Involved?**

The potentially impacted information includes your full name and the following: <<b2b\_text\_2 (Exposed Data Elements)>>.

### **What You Can Do**

While we have no evidence of financial fraud or identity theft related to this data, we want to make you aware of the incident. Out of an abundance of caution, and to help protect you from potential misuse of your information, we have secured the services of Kroll to provide identity monitoring at no cost to you for <<ServiceTerminMonths>> months. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration. Enrolling in this program will not hurt your credit score. For more information, including instructions on how to activate your complimentary membership, please see the additional information provided below in the section titled, "Other Important Information."

This letter also provides 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 personal information on the following pages.

**For More Information**

DBR & CO is committed to maintaining the privacy of personal information in our possession and has taken many precautions to safeguard it. We also 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 (844) 576-3122, Monday through Friday from 8:00 am to 5:30 pm Central Time, excluding major US holidays. This response line is staffed with professionals familiar with this incident and knowledgeable on what you can do to protect against potential misuse of your information.

Sincerely,

**DBR & CO**

436 Seventh Avenue, Suite 2800, Pittsburgh, PA 15219

– OTHER IMPORTANT INFORMATION –

**1. Enrolling in Complimentary <<ServiceTerminMonths>>-Month Identity Monitoring.**

To help protect your identity, we are offering complimentary access to Kroll identity monitoring services for <<ServiceTerminMonths>> months.

**How to Activate Your Monitoring Services**

1. You must activate your services by <<b2b\_text\_6 (Date)>>. Your Activation Code will not work after this date.
2. Visit <https://enroll.krollmonitoring.com> to activate your identity monitoring services.
3. Provide Your Membership Number: <<Member ID (S\_N)>>

**Take Advantage of Your Monitoring Services**

You've been provided with access to the following services from Kroll:

**Single Bureau Credit Monitoring.** You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who can help you determine if it's an indicator of identity theft. To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

**Fraud Consultation.** You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

**Identity Theft Restoration.** If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to an investigator who understands your issues and can do most of the work for you. Your investigator can dig deep to uncover the scope of the identity theft, and then work to resolve it.

**2. Protecting Your Medical Information.**

We have no evidence that your medical information involved in this incident was or will be used for any unintended purposes. However, 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.

**3. 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 30348-5069  
<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

#### **4. Placing a Security Freeze on Your Credit File.**

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.

#### **5. Obtaining a Free Credit Report.**

Under federal law, you are entitled to one (1) free credit report every twelve (12) months from each of the above three (3) major nationwide credit reporting companies. Call **1-877-322-8228** or request your free credit reports online at **[www.annualcreditreport.com](http://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.

#### **6. 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](http://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.

**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.

**Massachusetts Residents:** Under Massachusetts law, you have the right to obtain a police report in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

**New Mexico Residents:** You have rights under the federal Fair Credit Reporting Act (FCRA). These include, among others, the right to know what is in your file; to dispute incomplete or inaccurate information; and to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, please visit [www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf](http://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf) or [www.ftc.gov](http://www.ftc.gov).

**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/](http://www.ncdoj.gov/), Telephone: 877-566-7226 (Toll-free within North Carolina), 919-716-6000.

**Oregon Residents:** You may obtain information about preventing identity theft from the Oregon Attorney General's Office: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, [www.doj.state.or.us/](http://www.doj.state.or.us/), Telephone: 877-877-9392.

**Rhode Island Residents:** You may contact law enforcement, such as the Rhode Island Attorney General's Office, to report incidents of identity theft or to learn about steps you can take to protect yourself from identity theft. You can contact the Rhode Island Attorney General at: Rhode Island Office of the Attorney General, 150 South Main Street, Providence, RI 02903, [www.riag.ri.gov](http://www.riag.ri.gov), 401-274-4400. There were 2 Rhode Island residents impacted by this incident.

**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.