

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

September 9, 2021

**VIA U.S. MAIL**

Attorney General John Formella  
Office of the Attorney General  
33 Capitol Street  
Concord, NH 03301

**Re: DC Group – Incident Notification**

Dear Mr. Formella:

McDonald Hopkins PLC represents DC Group. I am writing to provide notification of an incident at DC Group that may affect the security of personal information of approximately four (4) New Hampshire residents. DC Group'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, DC Group does not waive any rights or defenses regarding the applicability of New Hampshire law or personal jurisdiction.

DC Group recently discovered unauthorized access to its network occurred between April 11, 2021 and May 4, 2021. DC Group immediately launched an investigation in consultation with outside cybersecurity professionals who regularly investigate and analyze these types of situations to analyze the extent of any compromise of the information on the network. Based on its comprehensive investigation and document review, which concluded on August 11, 2021, DC Group discovered that the affected residents' full names and one (1) or more of the following may have been removed from the network in connection with this incident: Social Security numbers, driver's license numbers, and/or government-issued identification numbers.

To date, DC Group is not aware of any reports of identity fraud or improper use of any information as a direct result of this incident. Nevertheless, out of an abundance of caution, DC Group 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. DC Group is providing the affected residents with written notification of this incident commencing on or about September 10, 2021, in substantially the same form as the letter attached hereto. DC Group is offering the affected residents complimentary one-year memberships with a credit monitoring service. DC Group 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.

RECEIVED

SEP 13 2021

CONSUMER PROTECTION

September 9, 2021  
Page 2

At DC Group, protecting the privacy of personal information is a top priority. DC Group is committed to maintaining the privacy of personal information in its possession and has taken many precautions to safeguard it. DC Group continually evaluates and modifies its practices and internal controls to enhance the security and privacy of personal information.

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

Very truly yours,



Colin M. Battersby

Encl.

uninterrupted power



Return Mail Processing Center  
P.O. Box 6336  
Portland, OR 97228-6336

[REDACTED]

[REDACTED]

[REDACTED]

Dear [REDACTED]

I am writing with important information regarding a recent security incident. The privacy and security of the personal information we maintain is of the utmost importance to DC Group. We wanted 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?

We recently discovered unauthorized access to our network occurred between April 11, 2021 and May 4, 2021.

What We Are Doing.

We immediately launched an investigation in consultation with outside cybersecurity professionals who regularly investigate and analyze these types of situations to analyze the extent of any compromise of the information on our network.

What Information Was Involved?

Based on our comprehensive investigation and document review, which concluded on August 11, 2021, we discovered that your full name and one or more of the following may have been removed from our network in connection with this incident: [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. 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 you a one-year membership in myTrueIdentity provided by TransUnion Interactive, a subsidiary of TransUnion. For more information on identity theft prevention and myTrueIdentity, including instructions on how to activate your 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.

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 Monday through Friday, 9AM to 9PM EST.

Sincerely,

DC Group

- OTHER IMPORTANT INFORMATION -

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

As a safeguard, we have arranged for you to enroll, at no cost to you, in an online credit monitoring service (myTrueIdentity) for one year provided by TransUnion Interactive, a subsidiary of TransUnion®, one of the three nationwide credit reporting companies.

To enroll in this service, go to the myTrueIdentity website at [www.mytrueidentity.com](http://www.mytrueidentity.com) and in the space referenced as "Enter Activation Code", enter the following 12-letter Activation Code [REDACTED] and follow the three steps to receive your credit monitoring service online within minutes.

You can sign up for the online credit monitoring service anytime between now and [REDACTED]. Due to privacy laws, we cannot register you directly. Please note that credit monitoring service might not be available for individuals who do not have a credit file with TransUnion, or an address in the United States (or its territories) and a valid Social Security number. Enrolling in this service will not affect your credit score.

Once you are enrolled, you will be able to obtain one year of unlimited access to your TransUnion credit report and credit score. The daily credit monitoring service will notify you if there are any critical changes to your credit file at TransUnion, including fraud alerts, new inquiries, new accounts, new public records, late payments, change of address and more. The service also includes access to an identity restoration program that provides assistance in the event your identity is compromised to help you restore your identity and up to \$1,000,000 in identity theft insurance with no deductible. (Policy limitations and exclusions may apply.)

If you believe you may be a victim of identity theft, please call the toll-free TransUnion Fraud Response Services hotline at [REDACTED]. When prompted, enter the following 6-digit telephone pass code [REDACTED] to speak to a TransUnion representative about your identity theft issue.

**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 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**

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

<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

<https://www.equifax.com/personal/credit-report-services/credit-freeze/>

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 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](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.