

Dominic A. Paluzzi  
Direct Dial: 248.220.1356  
E-mail: [dpaluzzi@mcdonaldhopkins.com](mailto:dpaluzzi@mcdonaldhopkins.com)

August 31, 2021

**VIA U.S. MAIL**

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

**Re: Career Group, Inc. – Incident Notification**

Dear Mr. Formella:

McDonald Hopkins PLC represents Career Group, Inc. (“Career Group”). I am writing to provide notification of an incident that may affect the security of personal information of nineteen (19) New Hampshire residents. Career 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, Career Group does not waive any rights or defenses regarding the applicability of New Hampshire law or personal jurisdiction.

On July 2, 2021, Career Group detected potential unauthorized access to its network. Upon learning of this issue, Career Group contained and secured the threat, commenced a prompt and thorough investigation, and notified law enforcement. Career Group immediately launched an investigation in consultation with outside cybersecurity professionals to help determine whether any sensitive data had been compromised because of the incident. Career Group’s investigation determined that the unauthorized individual(s) potentially removed certain files and folders from portions of its network between June 28, 2021 and July 7, 2021. On August 6, 2021, following an extensive review and analysis of the data at issue, Career Group determined that certain files and folders potentially removed from its network contained the residents’ full name and Social Security number.

At the time of this notification, Career Group is not aware of any reports of identity theft or fraud arising out of this incident. Nevertheless, out of an abundance of caution, Career 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. Career Group is providing the affected residents with written notification of this incident commencing on or about August 31, 2021 in substantially the same form as the letter attached hereto. Career Group is offering the affected residents complimentary one-year membership with a credit monitoring service. Career Group will advise the affected residents to always remain vigilant in reviewing financial account statements for fraudulent or irregular activity on a regular basis. Career Group will advise the affected residents about the process for placing a fraud alert and/or security freeze on their credit

August 31, 2021

Page 2

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

Should you have any questions regarding this notification, please contact me at (248) 220-1356 or [dpaluzzi@mcdonaldhopkins.com](mailto:dpaluzzi@mcdonaldhopkins.com). Thank you for your cooperation.

Very truly yours,



Dominic A. Paluzzi

Encl.

CAREERGROUPCOMPANIES

Dear [REDACTED]

We are 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 Career Group Companies. 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 personal information.

What Happened?

On July 2, 2021, Career Group Companies detected potential unauthorized access to its network.

What We Are Doing

Upon learning of this issue, we contained and secured the threat, commenced a prompt and thorough investigation, and notified law enforcement. We immediately launched an investigation in consultation with outside cybersecurity professionals who regularly investigate and analyze these types of situations to help determine whether any sensitive data had been compromised because of the incident. Our investigation determined that the unauthorized party potentially removed certain files and folders from portions of our network between June 28, 2021 and July 7, 2021. We received assurances from the unauthorized party that the data removed from our environment was permanently deleted and not further disseminated.

What Information Was Involved

On August 6, 2021, following an extensive review and analysis of the data at issue, we determined that certain files and folders potentially removed from our network contained your [REDACTED]. Given the unauthorized network access, potential acquisition of certain files and the value we place on our relationship with you, we wanted to notify you about this incident.

What You Can Do

To date, we are not aware of any reports of identity theft arising out of this incident. Nevertheless, out of an abundance of caution, we want to make you aware of the incident. To protect you from potential misuse of your information, we are offering a complimentary one-year membership of Experian IdentityWorks<sup>SM</sup> 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 Security Freeze on your credit files, and 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, 8:00 am to 5:30 pm Central Time.**

Sincerely,

[REDACTED]  
Career Group, Inc.

– 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.
- **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 <https://www.experianidworks.com/3bcredit>  
or call 877-288-8057 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](http://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 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 LLC*

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.

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.

**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.

**Iowa Residents:** You may contact law enforcement or the Iowa Attorney General's Office to report suspected incidents of identity Theft: Office of the Attorney General of Iowa, Consumer Protection Division, Hoover State Office Building, 1305 East Walnut Street, Des Moines, IA 50319, [www.iowaattorneygeneral.gov](http://www.iowaattorneygeneral.gov), Telephone: (515) 281-5164

**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, [www.oag.state.md.us/Consumer](http://www.oag.state.md.us/Consumer), Telephone: 1-888-743-0023.

**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, Department of Justice, 9001 Mail Service Center, Raleigh, NC 27699-9001, [www.ncdoj.gov/](http://www.ncdoj.gov/), Telephone: 877-566-7226.

**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