

Blair L. Dawson, FIP, CIPP/US, CIPP/E, CIPM
Direct Dial: 312-642-6131
E-mail: bdawson@mcdonaldhopkins.com

June 19, 2024

VIA Email (consumer@ag.iowa.gov)

Consumer Protection Division
Security Breach Notifications
Office of the Attorney General of Iowa
1305 E. Walnut Street
Des Moines, Iowa 50319-0106

Re: HireQuality – Incident Notification

To Whom This May Concern:

McDonald Hopkins PLC represents HireQuality Solutions LLC (“HireQuality”). I am writing to provide notification of an unauthorized access incident that may affect the security of personal information of approximately five hundred and six (506) Iowa residents. HireQuality’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, HireQuality does not waive any rights or defenses regarding the applicability of Iowa law or personal jurisdiction.

On December 7, 2023, HireQuality detected unauthorized access to a business email account, resulting in potential exposure of the data within the email communications. Upon learning of this issue, HireQuality contained the threat by disabling all unauthorized access to the network and immediately commenced a prompt and thorough investigation. As part of the investigation, HireQuality has been working very closely with external cybersecurity professionals experienced in handling these types of incidents. Following a forensics investigation, HireQuality discovered on May 7, 2024, that certain files that contain personal information were potentially removed from our network by the unauthorized party. HireQuality has confirmed this information impacted included the affected residents’ full names, Social Security numbers, financial account information, and date of birth. Not all data elements were impacted for each resident.

HireQuality has no indication that any information has been misused. Nevertheless, out of an abundance of caution, HireQuality wanted to inform you (and affected residents) of the incident and to explain the steps that it is taking to help safeguard the affected residents against identity fraud. HireQuality is providing affected residents with written notification of this incident, commencing on or about June 18, 2024, in substantially the same form as the letter attached hereto. HireQuality is offering the affected residents complimentary one-year membership with a credit monitoring service. HireQuality is also advising the affected residents

June 19, 2024

Page 2

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

If you have any additional questions, please contact me at (312) 642-6131 or bdawson@mcdonaldhopkins.com.

Very truly yours,

A handwritten signature in black ink, appearing to read 'BLD', with a long horizontal flourish extending to the right.

Blair L. Dawson, FIP, CIPP/US, CIPP/E, CIPM

Encl.

HireQuality Solutions, LLC

P.O. Box 989728

West Sacramento, CA 95798-9728

[REDACTED]

Enrollment Code: [REDACTED]

To Enroll, Scan the QR Code Below:



Or Visit:

<https://app.idx.us/account-creation/protect>

June 18, 2024

[REDACTED]

Dear [REDACTED]

HireQuality Solutions LLC (“HireQuality”) values and respects the privacy of the information entrusted to us, which is why we are writing to advise you of a security incident that may have involved your personal information. We have no reason to believe your information has been or will be misused for identity theft. Nonetheless, we want to provide you with details about the incident, explain the services we are making available to you, and let you know we continue to take significant measures to protect your information.

What Happened?

On or around December 7, 2023, HireQuality detected unauthorized access to a business email account, resulting in potential exposure of the data within the email communications.

What We Are Doing.

Upon learning of this issue, we contained the threat by disabling all unauthorized access to our network and 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. Following a forensics investigation, we discovered on May 7, 2023, that certain files that contain personal information were potentially removed from our network by the unauthorized party.

What Information Was Involved?

The impacted files contained some of your personal information. This included your name along with your [REDACTED].

What You Can Do.

We have no evidence that any of your information has been or will be misused for identity theft. However, to protect you from potential misuse of your information, we are offering a complimentary one-year membership of identity theft protection services through IDX, A ZeroFox Company, the data breach and recovery services expert. These services include credit and CyberScan monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed id theft recovery services. 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. The IDX services are completely free to you and enrolling in this program will not hurt your credit score. For more information on identity theft prevention

and identity protection services provided by IDX, including instructions on how to activate your complimentary one-year membership, please see the additional information provided in this letter. Please note the deadline to enroll is September 18, 2024.

Also provided in the “Other Important Information” portion of this letter are 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. In addition, if this letter indicates that your medical information was impacted, we have included steps you can take to protect health-related information.

For More Information

We value the trust you place in us to protect your privacy and apologize for any inconvenience or concern this incident might cause. **If you have any further questions regarding this incident, please call our toll-free response line at [REDACTED]** This response line is available Monday through Friday, from 8 am - 8 pm Central Time.

Sincerely,

HireQuality Solutions, LLC
302 W Broadway Street
PO Box 52
Polk City, IA 50226

OTHER IMPORTANT INFORMATION

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

To help protect your identity, we are offering a **complimentary [REDACTED]** membership of IDX identity theft protection services. This product helps detect possible misuse of your personal information and provides you with superior identity protection support focused on immediate identification and resolution of identity theft.

Website and Enrollment. Scan the QR image or go to [REDACTED] and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.

Activate the credit monitoring provided as part of your IDX identity protection membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.

2. Placing a Fraud Alert on Your Credit File.

Whether or not you choose to use the complimentary [REDACTED]-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) 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

3. 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/>
(800) 349-9960
(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 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.

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.

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, Telephone: 515-281-5164.