



Kris Kleiner
+1 720 566 4048
kkleiner@cooley.com

By Certified Mail Return Receipt Requested

September 28, 2018

Office of the New Hampshire Attorney General
Consumer Protection & Antitrust Bureau
33 Capitol Street
Concord, NH 03301

RECEIVED
OCT 01 2018
CONSUMER PROTECTION

Re: Legal Notice of Information Security Incident

Dear Sir or Madam:

I write on behalf of my client, Quest Nutrition, to inform you of a potential security incident involving the personal information of certain Quest Nutrition customers, which may have affected approximately two New Hampshire residents. Quest Nutrition is notifying potentially affected individuals and outlining some steps they may take to help protect themselves.

Quest Nutrition recently learned that an individual appears to have gained unauthorized access to a Quest Nutrition employee email account, which contained some personal information about certain employees, influencers/partners, and other individuals. Although Quest Nutrition cannot be certain whether any particular individual's information was accessed, because the information maintained in the account included certain personal information, such as names, addresses, usernames and passwords, driver's license information, medical or health insurance information, financial account information and Social Security number, this information could be affected by this incident. Accordingly, and out of an abundance of caution, Quest Nutrition is providing notice to potentially affected individuals and to your office in the event that any such information was viewed by an unauthorized person.

Quest Nutrition takes the privacy of personal information seriously and deeply regrets that this incident occurred. Upon learning of the incident, Quest Nutrition promptly took steps to address the situation, including initiating an internal investigation into this incident and retaining an independent forensic investigation firm to assist in their investigation of and response to this incident. Quest Nutrition has also reset all user account passwords and implemented additional email security tools to help prevent this type of incident from reoccurring in the future. Finally, Quest Nutrition has contacted law enforcement and will continue to cooperate in their investigation of this incident.

Potentially affected individuals are being notified starting on or around September 28, 2018. A form copy of the notice being sent to the potentially affected New Hampshire residents is included for your reference. If you have any questions or need further information regarding this incident, please contact me at (720) 566-4048 or kkleiner@cooley.com.



Office of the New Hampshire Attorney General
September 28, 2018
Page Two

Sincerely,

A handwritten signature in black ink, appearing to read "Kristopher Kleiner". The signature is written over a horizontal line and extends to the right.

Kristopher Kleiner

Enclosure



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

<<Mail ID>>
<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>>
<<Address 5>>
<<City>><<State>><<Zip>>
<<Country>>

<<Date>>

Notice of Data Breach

Dear <<Name1>>:

We are writing to inform you of a potential security incident involving certain personal information you provided to Quest Nutrition. We are providing this notice as a precaution to inform potentially affected individuals about the incident and to call your attention to some steps you can take to help protect yourself. We sincerely regret any concern this may cause you.

What Happened

We recently learned that an outside individual sent emails to certain Quest Nutrition employees soliciting their login information to our email system. The individual appears to have been able to use these credentials to gain unauthorized access to an employee email account, which contained certain personal information about a limited number of our employees, influencers/partners, and other individuals.

What Information Was Involved

The information stored in the affected email account varies by individual, but may include first and last name, address, username and password for certain online accounts, driver's license information, medical or health insurance information, financial account information and Social Security number. Based on our investigation, it appears you were one of the individuals whose information was stored in the account and therefore your information could be affected by this incident. Our investigation has not found any evidence that this incident involves any unauthorized access to or use of any of Quest Nutrition's internal computer systems or network, or that any customer information or any other employee or partner information was affected. Please note, at this time, we are not aware of any fraud or misuse of your information as a result of this incident.

What We Are Doing

We take the privacy of personal information seriously and deeply regret that this incident occurred. We took steps to address this incident promptly after it was discovered, including initiating an internal investigation into this incident and retaining an independent forensic investigation firm to assist us in our investigation of and response to this incident. Additionally, we have reset all user account passwords and implemented additional email security tools to help prevent this type of incident from reoccurring in the future.

To help protect your identity, we are offering one year of complimentary identity protection services from a leading identity monitoring services company. These services help detect possible misuse of your personal information and provide you with superior identity protection support focused on immediate identification and resolution of identity theft. For more information about these services and instructions on completing the enrollment process, please refer to the enrollment instructions included with this letter.

What You Can Do

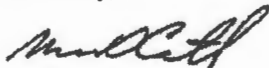
Although we are not aware of any identity theft arising out of this incident, we want to make you aware of steps that you can take as a precaution:

- **Activating the Complimentary Identity Protection Services.** As outlined above, we are offering one year of identity theft protection and credit monitoring services at no charge to you. For more information about these services and instructions on completing the enrollment process, please refer to the "Information about Identity Theft Protection" reference guide attached to this letter. Note that you must complete the enrollment process by **December 20, 2018**.
- **Checking Credit Reports and Financial Accounts.** You can carefully check your credit reports for accounts you did not open or for inquiries from creditors you did not initiate. If you see anything you do not understand, call the credit agency immediately. If you find any suspicious activity on your credit reports, call your local police or sheriff's office, and file a police report for identity theft and get a copy of it. You may need to give copies of the police report to creditors to clear up your records. You can also review your financial account statements to determine if there are any discrepancies or unusual activity listed. If you see anything you do not understand, call the financial institution immediately.
- **Change Account Passwords.** You should change the password to any accounts that may have been affected and, if you use the same or similar passwords with other online accounts, we recommend that you change your password for those accounts as well. You should use different and "strong" passwords for all accounts/websites. Tips on creating a strong password are available at <http://www.connectsafely.org/tips-to-create-and-manage-strong-passwords/>.
- **Reviewing Explanation of Benefits Documents.** You can also review explanation of benefits statements that you receive from your health insurer or health plan or review for persons whose medical bills you assist with or pay (such as your child). If you identify services listed on the explanation of benefits that were not received, please immediately contact your insurer or health plan.
- **Consulting the Identity Theft Protection Guide.** Finally, please review the "Information about Identity Theft Protection" reference guide, included here, which describes additional steps that you may wish to take to help protect yourself, including recommendations by the Federal Trade Commission regarding identity theft protection and details on placing a fraud alert or a security freeze on your credit file.

For More Information

For more information about this incident, or if you have additional questions or concerns, you may contact us at (855) 221-5660 between the hours of 6:00 a.m. and 6:00 p.m. Pacific time, Monday through Friday. Again, we sincerely regret any concern this incident may cause.

Sincerely,



Michael Castle,
Chief Financial Officer

Information about Identity Theft Protection

To help protect your identity, we are offering a complimentary membership in Experian's® IdentityWorks®. 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. Included with this service are fraud resolution services that provide an Experian Fraud Resolution agent to work with you to investigate and resolve each incident of fraud that occurred from the date of the incident (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition). While this Fraud Resolution assistance is immediately available to you without any further action on your part, you can also activate the fraud detection tools available through enrolling in IdentityWorks® at no cost to you. To enroll in these services, visit: www.experianidworks.com/3bcredit by **December 20, 2018**, and use the following activation code: <<ACTIVATION CODE>>. You may also enroll over the phone by calling **877-288-8057** between the hours of 9:00 AM and 9:00 PM (Eastern Time), Monday through Friday and 11:00 AM and 8:00 PM Saturday (excluding holidays). Please provide the following engagement number as proof of eligibility: **DB08652**.

Once you enroll in IdentityWorks, you will have access to the following features:

- **Experian credit report at signup:** See what information is associated with your credit file.
- **Active Surveillance Alerts:** Monitors Experian, Equifax and Transunion files for indicators of fraud.
- **Fraud Resolution:** Identity Theft Resolution agents are immediately available to help you address credit and non-credit related fraud.
- **ExtendCARE:** You receive the same high-level of Fraud Resolution support even after your IdentityWorks membership has expired.
- **\$1 Million Identity Theft Insurance¹:** Provides coverage for certain costs and unauthorized electronic fund transfers.

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.

Review Accounts and Credit Reports: You can regularly review statements from your accounts and periodically obtain your credit report from one or more of the national credit reporting companies. You may obtain a free copy of your credit report online at www.annualcreditreport.com, by calling toll-free 1-877-322-8228, or by mailing an Annual Credit Report Request Form (available at www.annualcreditreport.com) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. You may also purchase a copy of your credit report by contacting one or more of the three national credit reporting agencies listed at the bottom of this page.

You should remain vigilant with respect to reviewing your account statements and credit reports, and you should promptly report any suspicious activity or suspected identity theft to the proper law enforcement authorities, including local law enforcement, your state's attorney general, and/or the Federal Trade Commission ("FTC"). You may contact the FTC or your state's regulatory authority to obtain additional information about avoiding and protection against identity theft: Federal Trade Commission, Consumer Response Center 600 Pennsylvania Avenue, NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft.

For residents of Maryland: You may also obtain information about preventing and avoiding identity theft from the Maryland Office of the Attorney General: Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023, www.oag.state.md.us.

For residents of North Carolina: You may also obtain information about preventing and avoiding identity theft from North Carolina Attorney General's Office: North Carolina Attorney General's Office, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-5-NO-SCAM, www.ncdoj.gov.

For residents of Rhode Island: You may also obtain information about preventing and avoiding identity theft from the Rhode Island Office of the Attorney General: Rhode Island Office of the Attorney General, Consumer Protection Unit, 150 South Main Street, Providence, RI 02903, 401-274-4400, <http://www.riag.ri.gov>.

¹ 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.

Information About Medical Identity Theft: Patients who pay for medical services can regularly review the explanation of benefits (EOB) statements that they receive from their health insurers or health plans. If they identify services listed on the EOB that were not received, they should immediately contact the health plan. For more information about protecting yourself from the Department of Health and Human Services, please visit <https://oig.hhs.gov/fraud/medical-id-theft>.

Fraud Alerts: There are also two types of fraud alerts that you can place on your credit report to put your creditors on notice that you may be a victim of fraud: an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for at least 90 days. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. You can place a fraud alert on your credit report by contacting any of the three national credit reporting agencies at the addresses or toll-free numbers listed at the bottom of this notice.

Credit Freezes: You may have the right to put a credit freeze, also known as a security freeze, on your credit file, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate a freeze. A credit freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a credit freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a credit freeze may delay your ability to obtain credit. In addition, you may incur fees to place, lift and/or remove a credit freeze. Credit freeze laws vary from state to state. The cost of placing, temporarily lifting, and removing a credit freeze also varies by state, generally \$5 to \$20 per action at each credit reporting company. Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company. Since the instructions for how to establish a credit freeze differ from state to state, please contact the three major credit reporting companies as specified below to find out more information.

Additional Information for Massachusetts Residents: Massachusetts law gives you the right to place a security freeze on your consumer reports. The credit reporting company may charge a reasonable fee of up to \$5 to place a freeze or lift or remove a freeze, unless you are a victim of identity theft or the spouse of a victim of identity theft, and have submitted a valid police report relating to the identity theft to the credit reporting company. (By law, you have a right to obtain a police report relating to this incident, and if you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.) You may request that a freeze be placed on your credit report by sending a request to a credit reporting agency by certified mail, overnight mail or regular stamped mail to the address below. The following information should be included when requesting a security freeze (documentation for you and your spouse must be submitted when freezing a spouse's credit report): full name, with middle initial and any suffixes; Social Security number, date of birth (month, day and year); current address and previous addresses for the past five (5) years; and applicable fee (if any) or incident report or complaint with a law enforcement agency or the Department of Motor Vehicles. The request should also include a copy of a government-issued identification card, such as a driver's license, state or military ID card, and a copy of a utility bill, bank or insurance statement. Each copy should be legible, display your name and current mailing address, and the date of issue (statement dates must be recent).

Additional Information for New Mexico Residents: New Mexico Consumers Have the Right to Obtain a Security Freeze or Submit a Declaration of Removal. You may obtain a security freeze on your credit report to protect your privacy and ensure that credit is not granted in your name without your knowledge. You may submit a declaration of removal to remove information placed in your credit report as a result of being a victim of identity theft. You have a right to place a security freeze on your credit report or submit a declaration of removal pursuant to the Fair Credit Reporting and Identity Security Act.

The security freeze will prohibit a consumer reporting agency from releasing any information in your credit report without your express authorization or approval. The security freeze is designed to prevent credit, loans and services from being approved in your name without your consent. When you place a security freeze on your credit report, you will be provided with a personal identification number, password or similar device to use if you choose to remove the freeze on your credit report or to temporarily authorize the release of your credit report to a specific party or parties or for a specific period of time after the freeze is in place. To remove the freeze or to provide authorization for the temporary release of your credit report, you must contact the consumer reporting agency and provide all of the following:

- (1) the unique personal identification number, password or similar device provided by the consumer reporting agency;
- (2) proper identification to verify your identity;
- (3) information regarding the third party or parties who are to receive the credit report or the period of time for which the credit report may be released to users of the credit report; and
- (4) payment of a fee, if applicable.

A consumer reporting agency that receives a request from a consumer to lift temporarily a freeze on a credit report shall comply with the request no later than three business days after receiving the request. As of September 1, 2008, a consumer reporting agency shall comply with the request within fifteen minutes of receiving the request by a secure electronic method or by telephone.

A security freeze does not apply in all circumstances, such as where you have an existing account relationship and a copy of your credit report is requested by your existing creditor or its agents for certain types of account review, collection, fraud control or similar activities; for use in setting or adjusting an insurance rate or claim or insurance underwriting; for certain governmental purposes; and for purposes of prescreening as defined in the federal Fair Credit Reporting Act.

If you are actively seeking a new credit, loan, utility, telephone or insurance account, you should understand that the procedures involved in lifting a security freeze may slow your own applications for credit. You should plan ahead and lift a freeze, either completely if you are shopping around or specifically for a certain creditor, with enough advance notice before you apply for new credit for the lifting to take effect. You should contact a consumer reporting agency and request it to lift the freeze at least three business days before applying. As of September 1, 2008, if you contact a consumer reporting agency by a secure electronic method or by telephone, the consumer reporting agency should lift the freeze within fifteen minutes. You have a right to bring a civil action against a consumer reporting agency that violates your rights under the Fair Credit Reporting and Identity Security Act.

You can obtain more information about fraud alerts and credit freezes by contacting the FTC or one of the national credit reporting agencies listed below.

National Credit Reporting Agencies Contact Information

Equifax (www.equifax.com)

General Contact:

P.O. Box 740241
Atlanta, GA 30374
800-685-1111

Fraud Alerts:

P.O. Box 740256, Atlanta, GA 30374

Credit Freezes:

P.O. Box 105788, Atlanta, GA 30348

Experian (www.experian.com)

General Contact:

P.O. Box 2002
Allen, TX 75013
888-397-3742

Fraud Alerts and Security Freezes:

P.O. Box 9554, Allen, TX 75013

TransUnion (www.transunion.com)

General Contact:

P.O. Box 105281
Atlanta, GA 30348
800-888-4213

Fraud Alerts and Security Freezes:

P.O. Box 2000, Chester, PA 19022
888-909-8872