



Aubrey L. Weaver
550 E. Swedesford Road, Suite 270
Wayne, Pennsylvania 19087
Aubrey.Weaver@lewisbrisbois.com
Direct: 215.253.7506

October 11, 2022

VIA ONLINE SUBMISSION

Attorney General Aaron Frey
Maine Attorney General's Office
Consumer Protection Division
6 State House Station
Augusta, ME 04333

Re: Notice of Data Security Incident

Dear Attorney General Frey:

We represent The Quest Group, a cable and audio products manufacturer located in California. This letter is being sent because personal information belonging to certain current and former The Quest Group employees may have been involved in a recent data security incident, including a resident of Maine. The potentially affected information included the resident's name, Social Security number, other government ID number, and/or health insurance information.

On August 17, 2022, The Quest Group learned of unusual activity impacting certain computer systems and discovered evidence consistent with ransomware encryption. At that time, The Quest Group launched an investigation with the assistance of a leading independent computer forensics firm to determine what happened and whether personal information may have been involved. On August 28, 2022, when the forensic investigation concluded, The Quest Group learned that certain administrative files may have been acquired without authorization. Thereafter, The Quest Group launched a comprehensive review of those files to identify whether any sensitive information was contained therein. On September 9, 2022, The Quest Group identified one (1) potentially affected Maine resident whose information may have been involved.

The Quest Group notified the potentially affected Maine resident of this incident via U.S. Mail on October 7, 2022. In so doing, The Quest Group offered notified individuals one year of complimentary identity protection services through Kroll. These services include Credit Monitoring, \$1 Million Identity Fraud Loss Reimbursement, Fraud Consultation, and Identity Theft Restoration. A sample copy of the notification letter is attached to this correspondence.

October 11, 2022
Page 2

The Quest Group takes the privacy and security of all information in its possession very seriously. If you have any questions or need additional information, please do not hesitate to contact me at (215) 253-7506 or Aubrey.Weaver@lewisbrisbois.com.

Sincerely,

A handwritten signature in black ink, appearing to read 'Aubrey L. Weaver', with a stylized flourish at the end.

Aubrey L. Weaver of
LEWIS BRISBOIS BISGAARD & SMITH LLP

Enc.: Sample Consumer Notification Letter



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

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country>>

<<b2b_text_1(Subject: Notice of Data [Security Incident/Breach])>>

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

I am writing to inform you of a data security incident that may have affected your personal information. At The Quest Group dba AudioQuest and Golden Ear, we take the privacy and security of personal information very seriously. We are contacting you to notify you that this incident occurred and inform you about steps you can take to ensure your information is protected, including activating the complimentary identity monitoring services we are making available to you.

What Happened? On August 17, 2022, The Quest Group learned of unusual activity impacting certain computer systems and discovered evidence consistent with ransomware encryption. Upon discovering this activity, we immediately launched an investigation with the assistance of a leading independent computer forensics firm to determine what happened and whether personal information may have been involved. The forensic investigation concluded on August 28, 2022, and determined that certain administrative files from The Quest Group may have been acquired without authorization on August 17, 2022. We then launched a comprehensive review of those files to identify any sensitive information that may have been contained therein. On September 9, 2022, we learned that some of your information was contained within the potentially affected data.

What Information Was Involved? The affected information may have included your <<b2b_text_2(data elements)>>.

What Are We Doing? As soon as we discovered this incident, we took the steps described above. We have also implemented additional safeguards to help ensure the security of our network environment and to reduce the risk of a similar incident occurring in the future.

To help relieve concerns and to help protect your identity following this incident, The Quest Group has secured the services of Kroll to provide credit monitoring and identity theft restoration services at no cost to you for 12 months. Kroll is a global leader in risk mitigation and response, and the Kroll team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Web Watcher, \$1 Million Identity Fraud Loss Reimbursement, Fraud Consultation, and Identity Theft Restoration.

Visit <https://enroll.krollmonitoring.com> to activate and take advantage of your identity monitoring services.

You have until <<b2b_text_6(activation deadline)>> to activate your identity monitoring services.

Membership Number: <<Membership Number s_n>>

What Can You Do? We recommend that you review the guidance included with this letter about how to help protect your information. The Quest Group also encourages you to take full advantage of the services offered to you through Kroll. Kroll representatives are available to answer questions or address concerns you may have regarding protection of your information. Kroll call center representatives are available Monday through Friday from 6:00 am – 3:30 pm Pacific Time and can be reached by calling 1-???-???-????.

For More Information: Further information about how to help protect your personal information appears on the following page. If you have questions or need assistance, please call [1-800-833-8333](tel:1-800-833-8333), Monday through Friday from 6:00 am – 3:30 pm Pacific Standard Time, excluding some major U.S. holidays.

We take your trust in us and this matter very seriously. Please accept our sincere apologies for any worry or inconvenience that this may cause you.

Sincerely,

A handwritten signature in black ink, appearing to read "Mike McConnell". The signature is fluid and cursive, with the first name "Mike" being more prominent than the last name "McConnell".

Mike McConnell, Chief Financial Officer

The Quest Group
2621 White Road
Irvine, CA 92614

Steps You Can Take to Protect Your Personal Information

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (FTC).

Copy of Credit Report: You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting <http://www.annualcreditreport.com/>, calling toll-free 1-877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You also can contact one of the following three national credit reporting agencies:

Equifax

P.O. Box 105851
Atlanta, GA 30348
1-800-525-6285
www.equifax.com

Experian

P.O. Box 9532
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion

P.O. Box 2000
Chester, PA 19016
1-800-916-8800
www.transunion.com

Fraud Alert: You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least one year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at <http://www.annualcreditreport.com>.

Security Freeze: You have the right to put a security freeze on your credit file for up to one year at no cost. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC, or from your respective state Attorney General about fraud alerts, security freezes, and steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the Attorney General in your state.

Federal Trade Commission

600 Pennsylvania Ave, NW
Washington, DC 20580
consumer.ftc.gov, and
www.ftc.gov/idtheft
1-877-438-4338

Maryland Attorney General

200 St. Paul Place
Baltimore, MD 21202
oag.state.md.us
1-888-743-0023

New York Attorney General

Bureau of Internet and
Technology Resources
28 Liberty Street
New York, NY 10005
1-212-416-8433

North Carolina Attorney General

9001 Mail Service Center
Raleigh, NC 27699
ncdoj.gov
1-877-566-7226

Rhode Island Attorney General

150 South Main Street
Providence, RI 02903
<http://www.riag.ri.gov>
1-401-274-4400

Washington D.C. Attorney General

441 4th Street, NW
Washington, DC 20001
oag.dc.gov
1-202-727-3400

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include to know what is in your file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information; as well as other rights. For more information about the FCRA, and your rights pursuant to the FCRA, please visit <https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf>.



TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You have 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 will be able to help you determine if it is an indicator of identity theft.

Web Watcher

Web Watcher monitors internet sites where criminals may buy, sell, and trade personal identity information. An alert will be generated if evidence of your personal identity information is found.

\$1 Million Identity Fraud Loss Reimbursement

Reimburses you for out-of-pocket expenses totaling up to \$1 million in covered legal costs and expenses for any one stolen identity event. All coverage is subject to the conditions and exclusions in the policy.

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 a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge.

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.