LEWIS BRISBOIS BISGAARD & SMITH LLP

Allen E. Sattler
650 Town Center Drive, Suite 1400
Costa Mesa, California 92626
Allen.Sattler@lewisbrisbois.com
Direct: 714.668.5572

December 31, 2020

File No. 36629.141

VIA EMAIL

Washington Office of the Attorney General
1125 Washington St SE
PO Box 40100
Olympia, WA 98504
Email: SecurityBreach@atg.wa.gov

Re: Notification of Data Security Incident

Dear Washington Office of the Attorney General:

Lewis Brisbois Bisgaard & Smith LLP represents Life Quotes, Inc. ("Life Quotes") in connection with a recent data security incident described in greater detail below. The purpose of this letter is to notify you of the incident in accordance with Washington's data breach notification statute, RCW 19.255.010.

1. Nature of the Security Incident

Life Quotes is an insurance broker headquartered in Darien, Illinois.

On October 20, 2020, Life Quotes discovered that its Windows-based systems had been encrypted as a result of a ransomware attack. A ransom note found on one of the affected servers identified Conti as the ransomware variant. Because Life Quotes' cloud-based back up files were available, Life Quotes restored its systems from such backup files and did not establish communications with the threat actor.

On November 20, 2020, several members of Life Quotes' leadership team received an email from the threat actor. The email claimed that the threat actor obtained files from Life Quotes environment and plans to publish such files unless Life Quotes initiates negotiations by November 23, 2020. Following the receipt of this email, Life Quotes retained a cybersecurity and digital forensics firm and incident response counsel to assist with its response efforts.

On November 23, 2020, the cybersecurity and digital forensics firm established communications with the threat actor. Life Quotes ultimately did not reach a resolution on the ransom payment with the threat actor.

The forensic investigation to determine the source of the compromise and the scope of the incident is currently on-going.

2. Type of Information and Number of Washington Residents Involved

The incident involved personal information for approximately 612 Washington residents. The information involved in the incident may differ depending on the individual but may include name, address, date of birth, Social Security number, driver's license or state identification number, financial account information, and credit/debit card information. For a small subset of these individuals, the information involved also included health information

The affected individuals will receive a letter notifying them of the incident, offering complimentary identity monitoring services, and providing additional steps they can take to protect their personal information. The notification letters will be sent via USPS First Class Mail on December 31, 2020.

3. Measures Taken to Address the Incident

In response to the incident, Life Quotes retained cybersecurity experts and launched a forensics investigation to determine the source and scope of the compromise. Life Quotes is in the process of implementing additional security measures to further harden its digital environment in an effort to prevent a similar event from occurring in the future.

In addition, Life Quotes has reported the incident to the Darien police department and the Federal Bureau of Investigation ("FBI") and will cooperate fully to assist with any investigation. Furthermore, Life Quotes has notified the Washington Office of the Insurance Commissioner. It will also notify nationwide credit reporting agencies of the incident if appropriate.

As discussed above, Life Quotes is notifying the affected individuals and providing them with steps they can take to protect their personal information, including enrolling in the complimentary identity monitoring services offered in the notification letter.

4. Contact Information

Life Quotes is dedicated to protecting the sensitive information within its control. If you have any questions or need additional information regarding this incident, please do not hesitate to contact Allen Sattler at 714-668-5572 or Allen.Sattler@lewisbrisbois.com.

Sincerely,

Allen E. Sattler of
LEWIS BRISBOIS BISGAARD & SMITH LLP

AES

Encl.: Sample Consumer Notification Letter

cc: Jennifer Lee, Lewis Brisbois (Jennifer.Lee@lewisbrisbois.com)
Vy Nguyen, Lewis Brisbois (Vy.Nguyen@lewisbrisbois.com)

LifeQuotes.com
Over 380,000 Customers Insured
8205 South Cass Ave., Suite 102, Darien, IL 60561

December 31, 2020

To Enroll Visit:
https://www.cs4protect.com

Access Code: **274HQ207512**

«Name»
«Street_Address»
«City», «State» «Zip»

Dear «Name»:

I am writing to inform you of a recent data security incident experienced by Life Quotes, Inc. that may have involved your personal information. Please read carefully as this letter contains background information about the incident, the type of information involved, and steps you can take to protect your personal information.

What Happened: On October 20, 2020, Life Quotes learned that its systems had been encrypted as a result of a ransomware attack. Upon discovery, we took immediate steps to secure our systems prior to restoration. In addition, we retained outside cybersecurity experts to conduct an investigation to determine the source and scope of the incident.

The forensic investigation revealed that an unauthorized third party had access to our network on October 19, 2020 and October 20, 2020. Based the findings from the investigation, we reviewed the affected systems to determine the personal information that may have been impacted as a result of the incident, the individuals to whom the information pertained, and addresses for these individuals. On December 1, 2020, we determined that the affected systems contained some of your personal information.

What Information Was Involved: The information involved varies depending on the individual, but it may include the following: «Data_Exposed».

What We Are Doing: As soon as we learned of the incident, we immediately began containment, mitigation, and restoration efforts. We also launched an investigation and engaged outside cybersecurity experts to assist us in determining what happened. As part of the response processes, we implemented additional security measures to further harden our digital environment in an effort to prevent a similar event from occurring in the future.

In addition, we have reported the incident to law enforcement agencies, including the Federal Bureau of Investigation, and are committed to providing the FBI and law enforcement whatever assistance is needed. We have notified regulatory agencies and credit reporting agencies as well.

Furthermore, we are providing you with information about steps that you can take to help protect your personal information, and as an added precaution, we are offering you 12 months of complimentary credit and identity monitoring services through CyberScout. These services will provide you with alerts when changes occur to your Experian credit file or if your personal information is found on the dark web. To enroll, please log on to:

https://www.cs4protect.com

When prompted please input the following Access Code to register and authenticate to receive services: **274HQ207512**

The deadline to enroll is **March 31, 2021**.

What You Can Do: You can enroll in the complimentary credit and identity monitoring services offered in this letter. In addition, you can review the resources provided on the following page for additional steps to protect your personal information.

For More Information: If you have any questions regarding the incident or would like assistance with enrolling in the credit and identity monitoring services, please call **800-331-5242** between **9:00 a.m. and 9:00 p.m. Eastern Time, Monday Through Friday**.

The security of your information is a top priority for Life Quotes, and we are committed to safeguarding your data and privacy.

Sincerely,

Bob Bland
CEO, Life Quotes, Inc.

* Services marked with an "*" require an internet connection and e-mail account and may not be available to minors under the age of 18 years of age. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

Steps You Can Take to Further Protect Your 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 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 can print this form at https://www.annualcreditreport.com/cra/requestformfinal.pdf. You also can contact one of the following three national credit reporting agencies:

TransUnion	**Experian**	**Equifax**	**Free Annual Report**
P.O. Box 1000	P.O. Box 9532	P.O. Box 740241	P.O. Box 105281
Chester, PA 19016	Allen, TX 75013	Atlanta, GA 30374	Atlanta, GA 30348
1-800-916-8800	1-888-397-3742	1-800-525-6285	1-877-322-8228
www.transunion.com	www.experian.com	www.equifax.com	annualcreditreport.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 90 days. 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: Under U.S. law, 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. Residents of Maryland, North Carolina, and Rhode Island can obtain more information from their attorneys general using the contact information below.

Federal Trade Commission	**Maryland Attorney General**	**North Carolina Attorney General**	**Rhode Island Attorney General**
600 Pennsylvania Ave, NW	200 St. Paul Place	9001 Mail Service Center	150 South Main Street
Washington, DC 20580	Baltimore, MD 21202	Raleigh, NC 27699	Providence, RI 02903
www.consumer.ftc.gov	www.oag.state.md.us	www.ncdoj.gov	www.riag.ri.gov
www.ftc.gov/idtheft	1-888-743-0023	1-877-566-7226	401-274-4400
1-877-438-4338			

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include the right 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. For more information about the FCRA, and your rights pursuant to the FCRA, please visit http://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf.

Personal Information of a Minor: You can request that each of the three national credit reporting agencies perform a manual search for a minor's Social Security number to determine if there is an associated credit report. Copies of identifying information for the minor and parent/guardian may be required, including birth or adoption certificate, Social Security card, and government issued identification card. If a credit report exists, you should request a copy of the report and immediately report any fraudulent accounts to the credit reporting agency. You can also report any misuse of minor's information to the FTC at https://www.identitytheft.gov/. For more information about Child Identity Theft and instructions for requesting a manual Social Security number search, visit the FTC website: https://www.consumer.ftc.gov/articles/0040-child-identity-theft.

* Services marked with an "*" require an internet connection and e-mail account and may not be available to minors under the age of 18 years of age. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.