LEWIS BRISBOIS BISGAARD & SMITH LLP

Shelly L. Hall
550 West Adams Street, Suite 300
Chicago, Illinois 60661
Shelly.Hall@lewisbrisbois.com
Direct: 312.463.3362

April 6, 2022

**VIA ONLINE PORTAL**

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

Re: Notice of Data Security Incident

To Whom It May Concern:

Lewis Brisbois Bisgaard & Smith LLP represents Hidden Valley Insurance, Inc. ("Hidden Valley"), a full-service insurance agency based in Salt Lake City, Utah, in connection with a data security incident that may have affected the personal information belonging to Maine residents.

## 1) NATURE OF THE INCIDENT

Hidden Valley recently learned of unusual activity involving a Hidden Valley employee email account. Upon discovering this activity, Hidden Valley immediately took steps to secure its email system and engaged cybersecurity experts to assist with an investigation. The forensic investigation ultimately concluded that one (1) Hidden Valley employee email account may have been accessed without authorization on or about July 29, 2021. Hidden Valley promptly engaged a third-party vendor to assist with data mining and manual review of the contents of the identified account to determine whether any personal information may have been contained therein.

On March 14, 2022, Hidden Valley determined that personal information belonging to one (1) Maine resident was contained within the email account. The impacted information may have included the resident's driver's license number and/or state issued identification number. Hidden Valley then worked diligently to identify the current mailing addresses for each potentially impacted individual in order to notify them of the incident. To-date, Hidden Valley has no evidence that any potentially impacted information has been misused in conjunction with this incident.

## 2) NUMBER OF MAINE RESIDENTS IMPACTED

Hidden Valley notified the one Maine resident of this data security incident via first-class U.S. mail on April 4, 2021. A sample copy of the notification letter is attached hereto.

## 3) STEPS TAKEN RELATING TO THE INCIDENT

Hidden Valley has taken steps in response to this incident to enhance the security of personal information in its possession in an effort to prevent similar incidents from occurring in the future. These measures included: mandating password resets, implementing multi-factor authentication for all user accounts within its environment, as well as enabling unified audit logging features to detect any future suspicious activity within its email environment going forward.

While Hidden Valley has no indication that the information potentially affected by this incident has been misused, it nonetheless is providing individuals with information about steps that they can take to help protect their personal information.

## 4) CONTACT INFORMATION

Hidden Valley is committed to protecting the security of the personal information in their possession. Please feel free to contact me at Shelly.Hall@lewisbrisbois.com or by phone at (312) 463-3362 if you have any further questions.

Very truly yours,

Shelly L. Hall of
LEWIS BRISBOIS BISGAARD & SMITH LLP

Encl.: Sample Consumer Notification Letter

HIDDEN VALLEY
INSURANCE

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

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

**Re: Notice of Data Security Incident**

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

I am writing to inform you of a data security incident that may have involved your personal information. At Hidden Valley Insurance, we take the privacy and security of personal information in our possession very seriously. This is why we are writing to notify you of this incident and provide information on steps you can take to help protect your information.

**What Happened?** Hidden Valley Insurance recently learned of unusual activity involving an employee email account. Upon discovering this activity, we immediately began an investigation and took steps to secure our email system. We also engaged independent cybersecurity experts to conduct an investigation which revealed that the employee's email account may have been accessed without authorization on or about July 29, 2021. The investigation involved a search of the contents of the email account to identify whether any personal information was impacted and contact information for any affected individuals. That investigation concluded on February 25, 2022. On March 14, 2022, we learned that your personal information may have been impacted in connection with the incident which is the reason for this notification. Hidden Valley Insurance then worked diligently to identify address information required to effectuate this notification. Hidden Valley Insurance has no evidence of the misuse or attempted misuse of any potentially impacted information.

**What Information Was Involved?** The personal information potentially impacted by this incident, included your <<b2b_text_1 ("name" / Impacted Data)>>.

**What We Are Doing?** As soon as we discovered this incident, we took the measures referenced above. We are also providing you guidance on steps you can take to help protect your personal information as an added precaution.

**What Can You Do?** You can follow the recommendations included with this letter to help protect your information. Specifically, we recommend that you review your credit report for unusual activity. If you see anything that you do not understand or that looks suspicious, you should contact the consumer reporting agencies for assistance using the contact information included with this letter.

**For More Information:** If you have questions or need assistance, please contact Kroll at XXX-XXX-XXXX**.** Representatives are available to assist you Monday through Friday from 9:00 am – 6:30 pm Eastern Time, excluding major U.S. holidays. We have also provided more resources and contact information for agencies which can provide assistance in taking steps to further protect your information in the attached guidance included with this letter.

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

Sincerely,

Cheryl Blair
President
Hidden Valley Insurance, Inc.

## Additional 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 monitoring free credit reports closely for errors and by taking other steps appropriate to protect accounts, including promptly changing passwords. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained for remediation assistance or contact a remediation service provider. 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). You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the Federal Trade Commission is as follows:

*Federal Trade Commission*, Consumer Response Center
600 Pennsylvania Ave, NW, Washington, DC 20580
1-877-IDTHEFT (438-4338)
www.consumer.ftc.gov, www.ftc.gov/idtheft

**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:

- *Equifax*, P.O. Box 740241, Atlanta, GA 30374, 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 1000, Chester, PA 19016, 1-800-916-8800, www.transunion.com.

**Fraud Alerts:** There are two kinds of general fraud alerts you can place on your credit report—an initial alert and an extended alert. You may want to consider placing either or both fraud alerts 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. You may have an extended alert placed on your credit report if you have already been a victim of identity theft and provide the appropriate documentary poof. An extended fraud alert is also free and will stay on your credit report for seven years. 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. Military members may also place an Active Duty Military Fraud Alert on their credit reports while deployed. An Active Duty Military Fraud Alert lasts for one year and can be renewed for the length of your deployment

**Credit or Security Freezes:** Under U.S. law, you have the right to put a credit freeze, also known as a security freeze, on your credit file, for up to one year at no cost. The freeze 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. There is no fee to place or lift a security freeze. For information and instructions on how to place a security freeze, contact any of the credit reporting agencies or the Federal Trade Commission identified above. 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. After receiving your freeze request, each credit bureau will provide you with a unique PIN or password. Keep the PIN or password in a safe place as you will need it if you choose to lift the freeze.

A freeze remains in place until you ask the credit bureau to temporarily lift it or remove it altogether. If the request is made online or via phone, a credit bureau must lift the credit freeze within an hour. If the request is made by mail, then the bureau must lift the freeze no later than three business days after receiving your request.

**IRS Identity Protection PIN:** You can obtain an identity protection PIN (IP PIN) from the IRS that prevents someone else from filing a tax return using your Social Security number. The IP PIN is known only to you and the IRS and helps the IRS verify your identity when you file your electronic or paper tax return. You can learn more and obtain your IP PIN here: https://www.irs.gov/identity-theft-fraud-scams/get-an-identity-protection-pin.

**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.

**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.

**Additional Contact Information:**

**Maine:** Maine Attorney General can be reached at: 6 State House Station Augusta, ME 04333; 207-626-8800; https://www.maine.gov/ag/.

**Maryland:** Maryland Attorney General can be reached at: 200 St. Paul Place Baltimore, MD 21202; 1-888-743-0023; oag@state.md.us or IDTheft@oag.state.md.us

**North Carolina**: North Carolina Attorney General's Office, Consumer Protection Division, can be reached at: 9001 Mail Service Center Raleigh, NC 27699-9001; 877-5-NO-SCAM (Toll-free within North Carolina); 919-716-6000; www.ncdoj.gov

**New York**: New York Attorney General can be reached at: Bureau of Internet and Technology Resources, 28 Liberty Street, New York, NY 10005, 1-212-416-8433, https://ag.ny.gov/.

**Oregon**: Oregon Attorney General can be reached at: Office of the Attorney General, 1162 Court St. NE, Salem, OR 97301; 1-877-877-9392; https://www.doj.state.or.us/consumer-protection/

**Hidden Valley Insurance:** Hidden Valley Insurance can be reached via mail at PO Box 712450, Salt Lake City, Utah 84171-2450 and via phone at (801) 733-8500