March 23, 2021

Consumer Protection Bureau
Office of the Attorney General
33 Capitol Street
Concord, NH
03301

Re: Data Security Event: Public-Facing Web Quotes

Dear Attorney General MacDonald,

Hagerty Insurance Agency, LLC ("Hagerty"), pursuant to N.H. RSA § 359-C:20, is submitting this notice to provide the New Hampshire Attorney General with information regarding a suspected cybersecurity event involving unauthorized access to consumer personal information ("PI") potentially affecting 27 New Hampshire residents.

Hagerty maintains a public-facing website that includes an "Instant Quote" feature. Recent irregularities in traffic flow to our Instant Quote feature suggest that Hagerty may have been the target of the type of cyber fraud attack referenced in the Cyber Fraud Alert issued by the New York Department of Financial Services on February 16, 2021 ("the Fraud Alert").[1]

On February 2, Hagerty's web team noticed unusual quote activity consisting of a spike in unfinished quotes. Hagerty immediately launched an internal investigation but did not initially identify any signs of unauthorized access to PI. The initial findings revealed that these quotes were initiated by automatic means (aka "a Bot") and many were linked to deceased individuals. Hagerty suspected this was an attempt to scrape its website for corporate information, such as quote numbers or vehicle valuation data. On February 3, Hagerty's security team began blocking known IP addresses for the Bot(s).

As these attacks continued from new IP addresses, Hagerty's security team began using a rate limiter on its quote page and using a Captcha to stop Bot attacks.

Hagerty received the Fraud Alert on February 16. Hagerty then conducted a new review of the anomalous quote activity. With the information contained within the Fraud Alert, Hagerty was able to identify that PI was embedded in source code and therefore accessible. During the Instant Quote process, the user is required to enter limited personal data into the system, including name and date of birth, which Hagerty then supplements with related information pulled from LexisNexis to provide a quote.

The information involved for the approximately 27 New Hampshire residents is:

- Driver's License Number;
- Full Name;

[1] The Fraud Alert is available at https://www.dfs.ny.gov/industry_guidance/industry_letters/il20210216_cyber_fraud_alert.

- Date of Birth;
- Gender;
- Address;
- Marital Status; and
- This same information for other potential household drivers.

Accordingly, shortly after receiving the Fraud Alert and initiating a new investigation, at 4:00pm Eastern Time on February 16, Hagerty turned off its Instant Quote feature to stop these attacks. In addition, Hagerty took all NY DFS-recommended steps to secure data outlined in the Fraud Alert.

On February 23, Hagerty restored its web quote page with rate limiting, reCAPTCHA, and with measures designed to preclude personal information from being accessible through the webpage source code. In addition, Hagerty engaged a third party security specialist to conduct a penetration test to determine whether personal information remained accessible through the instant quote feature or anywhere else on Hagerty's public facing websites. On March 2, Hagerty discovered that despite these measures, personal information was still potentially accessible through its source code. As a precaution, Hagerty took back down its Instant Quote feature for further remediation and penetration testing. As of March 4, the Instant Quote feature is back on; but Hagerty is continuing to prevent any additional information from being pulled from LexisNexis to further ensure consumer information is protected. Since making these changes, the bot activity has diminished substantially.

Hagerty is also continuing its investigation to determine the full extent of the impact and any additional notifications that may be necessary. Hagerty plans to notify individuals as it concludes its investigation of who may have been affected, and it plans to provide free identity theft protection services. Individual notice letters are tentatively scheduled to be sent out on April 9. Hagerty also intends to notify consumer reporting agencies.

If you have any questions or require additional information, please contact me directly by phone at [redacted] or by email at [redacted]. Additionally, our physical mailing address is 121 Drivers Edge, Traverse City, MI 49684 should that be more convenient.

Cordially,

Michael Cole
Senior Privacy Counsel

March __, 2021

Re: Notice of Data Security Incident Involving Your Personal Data

Dear [Insert Name],

At Hagerty Insurance Agency, LLC ("Hagerty") we take data privacy very seriously. It is therefore important that we make you aware of any data privacy issues that may affect you. Below you will find information about an incident with our insurance quote feature that may have released your personal information without your authorization. We are actively taking steps to protect your information as outlined below. Please note that you may be affected even if you have no relationship with Hagerty.

Hagerty is an insurance agency specializing in providing specialty insurance for collectable vehicles. Hagerty maintains a public-facing website that includes an "Instant Quote" feature which allows anyone to obtain a tailored insurance quote for their vehicle by entering in basic personal information and details on the vehicle they want to insure. After personal information is entered, our quote feature tracks down additional consumer data from an outside provider for verification and to improve the accuracy of the automated quote.

What Happened

On February 2, Hagerty's web team noticed an increase in insurance quote requests via our "Instant Quote" feature. The high level of quote activity was suspicious and initial investigations indicated that automated "bots" were submitting fake quotes. Hagerty immediately deployed mechanisms to detect, prevent, and block bot activity in our quote system.

On February 16, Hagerty became aware that this incident was likely part of a widespread cyber-fraud scheme targeting quote systems across many different insurers and insurance agencies. Malicious bot activity is increasingly prevalent and can be used to tap into systems to harvest specific online consumer data. Based on information known about these widespread attacks, Hagerty was able to identify that the bot activity was intended to access individual's personal information, including driver's license numbers, that was inadvertently embedded in the source code of the quote webpage after submitting a request for a quote, and was therefore accessible to the attackers. While this additional personal information was not visible on the webpage itself, the attacker could search the source code to find it.

What Information Was Involved

Our records indicate that your name, driver's license number, and date of birth may have been accessed.

Actions We've Taken to Safeguard Your Information

We take our responsibility to safeguard your personal information as our utmost priority. We immediately deployed mechanisms to detect, prevent, and block bot activity in our quote feature and

have implemented processes and protocols to mitigate this type of activity. As of March 2nd, the quote feature safeguards have successfully prevented any additional bot activity.

Identify Theft Protection Service

To help protect your identity against the possibility that your information was compromised as part of this incident, we are offering complimentary access to Experian IdentityWorks^{SM} for 12 months. This product provides you with superior identity detection and resolution of identity theft. While identity restoration assistance is immediately available to you, we also encourage you to activate the fraud detection tools available through Experian IdentityWorks as a complimentary one-year membership.

To start monitoring your personal information, please follow the steps below:

- Ensure that you **enroll by: June 30, 2021** (Your code will not work after this date.)
- **Visit** Experian's website to enroll: https://www.experianidworks.com/credit
- Provide your **activation code:** [code]

Please do not share this information as these links are exclusive to you and your account.

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian's® IdentityWorks^{SM} online, please contact Experian's customer care team at (855) 726-7329 by June 30, 2021. Be prepared to provide engagement number DB26115 as proof of eligibility for the Identity Restoration services by Experian.

Steps You Can Take for Identity Theft Protection

We encourage you to take advantage of Experian's® IdentityWorks^{SM} identity theft protection services at no cost to you. In addition, there are other steps you may take to further protect yourself against identity theft or other unauthorized use of your personal information. Information regarding these steps is provided on the attached pages entitled *"Steps You May Take to Protect Yourself Against Potential Misuse of Information."*

Contact Information

We wanted you to know the nature and extent of this incident and to make you aware of the steps we are taking to protect your information. If you have questions about anything contained in this letter, please contact us by (855) 726-7329.

Regards,

Tony Grey
Vice President and Chief Information Security Officer

Steps You May Take to Protect Yourself Against Potential Misuse of Information

We recommend that you 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 obtain a copy of your credit report by contacting one or more of the three national credit reporting agencies listed below.

Equifax: P.O. Box 740241, Atlanta, Georgia 30374-0241, 1-800-685-1111, 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 19022, 1-800-888-4213, www.transunion.com

When you receive your credit reports, review them carefully. Look for accounts or creditor inquiries that you did not initiate or do not recognize. Look for information, such as home address and Social Security number, that is not accurate. If you see anything you do not understand, call the credit reporting agency at the telephone number on the report.

We recommend you remain vigilant with respect to reviewing your account statements and credit reports. We also recommend that you 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 identity theft.

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

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 7 years. You can place a fraud alert on your credit report by calling the toll-free fraud number of any of the three national credit reporting agencies listed below.

Equifax: 1-888-766-0008, www.equifax.com
Experian: 1-888-397-3742, www.experian.com
TransUnion: 1-800-680-7289, fraud.transunion.com

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. *Unlike a fraud alert, you must*

separately place a credit freeze on your credit file at each credit reporting company. Placing, lifting, and/or removing a credit freeze from your account is completely free and will not affect your credit score. Please contact the three national credit reporting agencies as specified below to find out more information:

Equifax:	P.O. Box 105788, Atlanta, GA 30348, www.equifax.com
Experian:	P.O. Box 9554, Allen, TX 75013, www.experian.com
TransUnion:	P.O. Box 2000, Chester, PA, 19022-2000, freeze.transunion.com

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

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 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).

For residents of the District of Columbia: You may also contact the District of Columbia Office of the Attorney General: Office of the Attorney General, Office of Consumer Protection, 400 6th Street, NW, Washington, DC 20001, (202) 442-9828, https://oag.dc.gov/.

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 New York: You may also obtain information about security breaches and preventing and avoiding identity theft from the New York Office of the Attorney General: Office of the Attorney General, The Capitol, Albany, NY 12224-0341, 1-800-771-7755, https://ag.ny.gov/.

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 Oregon: You may also contact the Oregon Office of the Attorney General: Oregon Department of Justice, 1162 Court St. NE, Salem, OR 97301-4096, 1-877-877-9392, help@oregonconsumer.gov, www.doj.state.or.us.

For residents of Rhode Island: You also may obtain information about preventing and avoiding identity theft from the Rhode Island Office of the Attorney General at: 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. You may also be able to file or obtain a police report about this incident.