ZwillGen

1900 M Street NW, Suite 250
Washington, DC 20036

Phone: (202) 296-3585
Website: www.zwillgen.com

April 15, 2021

Attorney General Gordon MacDonald
New Hampshire Department of Justice
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

Dear Attorney General MacDonald:

On behalf of our client, Government Employees Insurance Company ("GEICO"), we write to provide you with this notification of an incident that may have affected the personal information of New Hampshire residents.

GEICO recently became aware of a sophisticated attack on geico[.]com (the "Website"). On March 1, 2021, GEICO was alerted by an anonymous third-party researcher to the possible existence of a vulnerability in the Website, which purportedly allowed for the extraction of driver's license numbers. This responsible disclosure was immediately referred internally for investigation. GEICO's investigation revealed that hackers had submitted certain personal information about individuals – which they had obtained elsewhere – to begin the online sales quote process and then exploited a vulnerability in the Website that allowed for the extraction of the impersonated individuals' driver's license numbers. GEICO disabled the affected part of the system until a fix was implemented on the evening of March 1, 2021.

GEICO's investigation indicates that New Hampshire residents were targeted by the hackers between February 3, 2021 and March 1, 2021. The total number of New Hampshire license numbers subjected to unauthorized access through this attack is 166. While some of the affected individuals are current or former GEICO customers, many are not.

GEICO is committed to making appropriate adjustments to its security controls to help prevent future fraud and illegal activities on its websites. The company has devoted additional internal and external resources to further secure its sites in light of recent attacks on its online properties, including: (1) engaging two different data security vendors to independently review all external-facing applications to determine whether there are any other vulnerable code elements; (2) implementing page-specific alerting for anomalous behavior; (3) implementing additional client-side monitoring; and (4) implementing additional web application firewall measures to block access to specific code.

GEICO will begin to notify the individuals affected by this incident by mail beginning on April 9th and is offering them one year of complimentary identity theft protection services through IdentityForce. These services include Identity/Privacy Protection (fraud monitoring, dark web monitoring, dark web scan) and Identity Restoration (fully managed restoration, $1 million identity theft insurance). A copy of GEICO's notification letter is attached for your reference.

Should you have further questions about this matter, please do not hesitate to contact Paula Boston, Counsel for GEICO in the Office of the General Counsel, at PBoston@geico.com.

Sincerely,

Lynette Arce

Lynette Arce

GEICO

Consumer Privacy
750 Woodbury Road
Woodbury, NY 11797

April 09, 2021

[redacted]

NOTICE OF DATA BREACH

Dear [redacted],

We are writing to notify you of an incident that affected the confidentiality of your personal information. Please read this letter carefully for more information and to learn how you can take steps to protect your personal information.

What Happened?

We recently determined that between February 3, 2021 and March 1, 2021, fraudsters used information about you – which they acquired elsewhere – to obtain unauthorized access to your driver's license number through the online sales system on our website. We have reason to believe that this information could be used to fraudulently apply for unemployment benefits in your name. If you receive any mailings from your state's unemployment agency/department, please review them carefully and contact that agency/department if there is any chance fraud is being committed.

What Information Was Involved?

The data obtained by the fraudsters from GEICO was limited to your driver's license number.

What We Are Doing.

As soon as GEICO became aware of the issue, we secured the affected website and worked to identify the root cause of the incident. While we regularly maintain high security and privacy standards, we have also implemented—and continue to implement—additional security enhancements to help prevent future fraud and illegal activities on our website.

Although we don't know whether your driver's license number has been fraudulently used, we would like to offer you a one-year subscription to IdentityForce to help protect your identity from theft. If you would like to enroll in the IdentityForce identity-theft protection service, which includes Identity/Privacy Protection (fraud monitoring, dark web monitoring, and dark web scan) and Identity Restoration (fully managed restoration and $1 million identity theft insurance), please visit secure.identityforce.com/benefit/geico. You will need this one time use code to enroll: [redacted].

2000010000080052801000002

AN IMPORTANT MESSAGE REGARDING YOUR PERSONAL INFORMATION

What You Can Do.

In addition to enrolling in the IdentityForce services, we encourage you to be vigilant for incidents of fraud or identity theft by reviewing your account statements and credit reports for any unauthorized activity. There are additional actions you can consider taking to reduce the chances of identity theft or fraud on your account(s). Please see the attachment to this letter.

For More Information.

We apologize for any concern that this may have caused you. If you have any questions, please contact us at privacyrequests@geico.com or (855) 265-1097, Monday through Friday, 10 am to 6:30 pm EST.

Sincerely,

Sheila King
Manager, Data Privacy
GEICO Privacy Team

SUPPLEMENTAL INFORMATION

It is always advisable to be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting companies is as follows:

Equifax
P.O. Box 740241
Atlanta, GA 30374
www.equifax.com
1-800-685-1111

Experian
P.O. Box 2002
Allen, TX 75013
www.experian.com
1-888-397-3742

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

If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your state. You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. 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 Avenue NW
Washington, DC 20580
1-877-IDTHEFT (438-4338)
www.ftc.gov/idtheft

If you are a resident of California, Connecticut, Iowa, Maryland, Massachusetts, North Carolina, Oregon, or Rhode Island, you may contact and obtain information from and/or report identity theft to your state attorney general at:

California Attorney General's Office, California Department of Justice, Attn: Office of Privacy Protection, P.O. Box 944255, Sacramento, CA 94244-2550, (800) 952-5225

Connecticut Attorney General's Office, 55 Elm Street, Hartford, CT 06106, 1-860-808-5318, www.ct.gov/ag

Office of the Attorney General of Iowa, Hoover State Office Building, 1305 E. Walnut Street, Des Moines, IA 50319, (515) 281-5164, www.iowaattorneygeneral.gov

Maryland Attorney General's Office, 200 St. Paul Place, Baltimore, MD 21202, www.oag.state.md.us, 1-888-743-0023 or 1-410-576-6300

Office of the Massachusetts Attorney General, One Ashburton Place, Boston, MA 02108, 1-617-727-8400, www.mass.gov/ago/contact-us.html

North Carolina Attorney General's Office, 9001 Mail Service Center, Raleigh, NC 27699, www.ncdoj.gov, 1-919-716-6400 or 1-877-566-7226

Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, (503) 378-4400, http://www.doj.state.or.us/

Rhode Island Attorney General's Office, 150 South Main Street, Providence, RI 02903, 1-401-274-4400, www.riag.ri.gov

For other states: Information on how to contact your state attorney general may be found at www.naag.org/naag/attorneys-general/whos-my-ag.php.

2000010000080052801000004

If you are a resident of Massachusetts or Rhode Island , note that pursuant to Massachusetts or Rhode Island law, you have the right to file and obtain a copy of a police report. You also have the right to request a security freeze.

If you are a resident of West Virginia , you have the right to ask that nationwide consumer reporting agencies place "fraud alerts" in your file to let potential creditors and others know that you may be a victim of identity theft, as described below. You also have a right to place a security freeze on your credit report, as described below.

Fraud Alerts: There are two types of fraud alerts 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.

Credit Freezes: You have the right to put a credit freeze, also known as a security freeze, on your credit file, free of charge, so that no new credit can be opened in your name without the use of a PIN that is issued to you when you initiate a freeze. A security freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a security 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 security freeze may delay your ability to obtain credit.

There is no fee to place or lift a security freeze. Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit reporting company. For information and instructions to place a security freeze, contact each of the credit reporting agencies at the addresses below:

Experian Security Freeze	**TransUnion Security Freeze**	**Equifax Security Freeze**
P.O. Box 9554	P.O. Box 2000	P.O. Box 105788
Allen, TX 75013	Chester, PA 19016	Atlanta, GA 30348
www.experian.com/freeze/center.html	www.transunion.com/credit-freeze	my.equifax.com

To request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.)
2. Social Security number
3. Date of birth
4. If you have moved in the past five years, provide the addresses where you have lived over the prior five years
5. Proof of current address such as a current utility bill or telephone bill
6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.)
7. If you are a victim of identity theft, include a copy of the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

The credit reporting agencies have one business day after receiving your request by toll-free telephone or secure electronic means, or three business days after receiving your request by mail, to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within five business days and provide you with a unique personal identification number ("PIN") or password or both that can be used by you to authorize the removal or lifting of the security freeze.

To lift the security freeze in order to allow a specific entity or individual access to your credit report, or to lift a security freeze for a specified period of time, you must submit a request through a toll-free telephone number, a secure electronic means maintained by a credit reporting agency, or by sending a written request via regular, certified, or overnight mail to the credit reporting agencies and include proper identification (name, address, and Social Security number) and the PIN or password provided to you when you placed the security freeze as well as the identity of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have one business day after receiving your request by toll-free telephone or secure electronic means, or three business days after receiving your request by mail, to lift the security freeze for those identified entities or for the specified period of time.

To remove the security freeze, you must submit a request through a toll-free telephone number, a secure electronic means maintained by a credit reporting agency, or by sending a written request via regular, certified, or overnight mail to each of the three credit bureaus and include proper identification (name, address, and Social Security number) and the PIN number or password provided to you when you placed the security freeze. The credit bureaus have one business day after receiving your request by toll-free telephone or secure electronic means, or three business days after receiving your request by mail, to remove the security freeze.

Fair Credit Reporting Act: You also have rights under the federal Fair Credit Reporting Act, which promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. The FTC has published a list of the primary rights created by the FCRA (https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf), and that article refers individuals seeking more information to visit www.ftc.gov/credit. The FTC's list of FCRA rights includes:

- You have the right to receive a copy of your credit report. The copy of your report must contain all the information in your file at the time of your request.
- Each of the nationwide credit reporting companies – Equifax, Experian, and TransUnion – is required to provide you with a free copy of your credit report, at your request, once every 12 months.
- You are also entitled to a free report if a company takes adverse action against you, like denying your application for credit, insurance, or employment, and you ask for your report within 60 days of receiving notice of the action. The notice will give you the name, address, and phone number of the credit reporting company. You are also entitled to one free report a year if you're unemployed and plan to look for a job within 60 days; if you are on welfare; or if your report is inaccurate because of fraud, including identity theft.
- You have the right to ask for a credit score.
- You have the right to dispute incomplete or inaccurate information.
- Consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information.
- Consumer reporting agencies may not report outdated negative information.
- Access to your file is limited. You must give your consent for reports to be provided to employers.
- You may limit "prescreened" offers of credit and insurance you receive based on information in your credit report.
- You may seek damages from violators.
- Identity theft victims and active duty military personnel have additional rights.

In Addition, New Mexico Consumers Have the Right to Submit a Declaration of Removal. 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.

2000010000080052601000006