Clark Hill

July 27, 2023

VIA ELECTRONIC MAIL

Attorney General John Formella
Office of the Attorney General
33 Capitol Street
Concord, NH 03302
attorneygeneral@doj.nh.gov

Dear Attorney General Formella,

We represent Everest Global Services, Inc. ("Everest") as outside counsel with respect to a cybersecurity event, of which you were previously notified on or about December 16, 2022. Everest directly notified seven (7) New Hampshire residents of this incident on or about December 16, 2022. Everest concurrently notified employer/data owners whose employee information may have been affected, providing information about the incident, steps taken in response, and offering to provide notice to impacted individuals and state regulators on their behalf. As a result of this process, letters were mailed to an additional one (1) resident of New Hampshire via regular mail on or about February 6, 2023. Everest has previously notified you of these events.

During the initial notification process, Everest identified a number of records without addresses. Everest then had its vendor review the impacted data to identify additional data elements to assist with obtaining addresses. Once this process was complete, Everest used the additional data elements to search its claims system for addresses in order to notify impacted individuals directly. This process was recently completed, and on July 27, 2023, Everest notified an additional five (5) residents of New Hampshire via regular mail. A copy of the template notification letter is enclosed as Exhibit A. This completes the notification process, and Everest does not anticipate providing any further updates.

Please contact me if you have any questions.

Sincerely,

CLARK HILL

Melissa K. Ventrone
Member

cc: Sunaina Ramesh - sramesh@clarkhill.com

4145 SW Watson Avenue, Suite 400
Beaverton, OR 97005

July 27, 2023

NOTICE OF DATA SECURITY INCIDENT

Dear

We are writing to make you aware of a recent incident at Everest Global Services, Inc. ("Everest"), a reinsurance and insurance provider. Everest identified suspicious email activity and immediately took action to secure its email environment. **While your information was contained in one of the affected email accounts, we have no evidence that any of your personal information has been or will be misused. The security of your information is very important to us.** This letter contains more information about the proactive measures we have taken in response, as well the identity protection services that we are making available to you free of charge.

What Happened?

On August 15, 2022, Everest identified suspicious activity associated with its email environment. We immediately implemented our incident response protocols, took steps to secure the email environment, and engaged independent computer forensic experts to assist with an investigation. The investigation found that there was unauthorized access to five email accounts between August 8, 2022 and August 16, 2022. We conducted a thorough review of these accounts to identify any personal information present in the accounts during the unauthorized access. We learned on approximately October 10, 2022 that your information was present in a compromised account. Because we were not able to obtain your address from this process, we sought additional vendor assistance to locate additional information to enable us to search our claims system to do so. This was a manual, time intensive process which was only recently completed.

What Information Was Involved?

From our review, it appears that your may have been affected.

What We Are Doing:

Everest has taken proactive measures including resetting passwords for email accounts, reinforcing multi-factor authentication measures, and increasing the frequency of mandatory company-wide training and awareness of increasing cyber risks. In addition, we are offering identity theft protection services through IDX, the data breach and recovery services expert. IDX identity protection services include: of credit and CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed identity theft recovery services. **These services are being provided at no cost to you.** With this protection, IDX will help you resolve issues if your identity is compromised.

What You Can Do:

We encourage you to contact IDX with any questions and to enroll in free identity protection services by calling or going to and using the Enrollment Code provided above. IDX representatives are available Monday through Friday from 9 am - 9 pm Eastern Time. Please note the deadline to enroll is

You will find detailed instructions for enrollment on the enclosed Recommended Steps document. You will need to reference the enrollment code at the top of this letter when calling or enrolling online, so please do not discard this letter. We encourage you to take full advantage of this service offering. IDX representatives have been fully versed on the incident and can answer any questions or concerns regarding protection of your personal information. We also encourage you to vigilantly monitor your financial statements and credit reports and immediately report any suspicious activity.

For More Information:

If you have questions, please call Monday through Friday from 9 am - 9 pm Eastern Time. Protecting your information is important to us, and we sincerely apologize for any concern related to this incident.

Sincerely,

Everest Global Services, Inc.

Recommended Steps to Help Protect Your Information

1. **Website and Enrollment.** Go to and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.

2. Activate the credit monitoring provided as part of your IDX identity protection membership. **The monitoring included in the membership must be activated to be effective.** Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.

3. Telephone. Contact IDX at to gain additional information about this incident and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

4. Review your credit reports. We recommend that you remain vigilant by reviewing account statements and monitoring credit reports. Under federal law, you also are entitled every to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

If you discover any suspicious items and have enrolled in IDX identity protection, notify them immediately by calling or by logging into the IDX website and filing a request for help.

If you file a request for help or report suspicious activity, you will be contacted by a member of our ID Care team who will help you determine the cause of the suspicious items. In the unlikely event that you fall victim to identity theft as a consequence of this incident, you will be assigned an ID Care Specialist who will work on your behalf to identify, stop and reverse the damage quickly.

You should also know that you have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to your state Attorney General [or other consumer protection agency (contact information listed below)].

5. Place Fraud Alerts with the three credit bureaus. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. You can place a fraud alert at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. The contact information for all three bureaus is as follows:

Credit Bureaus

Equifax Fraud Reporting	Experian Fraud Reporting	TransUnion Fraud Reporting
1-866-349-5191	1-888-397-3742	1-800-680-7289
P.O. Box 105069	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348-5069	Allen, TX 75013	Chester, PA 19022-2000
www.equifax.com	www.experian.com	www.transunion.com

You need to contact only ONE of these bureaus and use only ONE of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well.

You will receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review. An initial fraud alert will last for one year.

Please Note: No one is allowed to place a fraud alert on your credit report except you.

6. Security Freeze. By placing a security freeze, you can prevent someone who fraudulently acquires your personal identifying information from using that information to open new accounts or borrow money in your name. You will need to contact **each of** the three national credit reporting bureaus listed above to place the freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card unless you temporarily lift or permanently remove the freeze. There is no cost to freeze or unfreeze your credit files.

7. You can obtain additional information about the steps you can take to avoid identity theft from the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

California Residents: Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft.

Kentucky Residents: Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601**,** www.ag.ky.gov, Telephone: 1-502-696-5300.

Maryland Residents: Office of the Attorney General of Maryland**,** Consumer Protection Division 200 St. Paul Place Baltimore, MD 21202**,** www.oag.state.md.us/Consumer, Telephone: 1-888-743-0023.

New Mexico Residents: You have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the 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 credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from a violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. You can review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

New York Residents: the Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; https://ag.ny.gov/.

North Carolina Residents: Office of the Attorney General of North Carolina**,** 9001 Mail Service Center Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 1-919-716-6400.

Oregon Residents: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 877-877-9392.

Rhode Island Residents: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 401-274-4400. A total of [xx] Rhode Island residents were notified of this incident.

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.gov/idtheft, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.