LEWIS BRISBOIS

LEWIS BRISBOIS BISGAARD & SMITH LLP

Sean B. Hoar
888 SW Fifth Avenue, Suite 900
Portland, OR 97204-2025
Sean.Hoar@lewisbrisbois.com
Direct: 971.712.2795

March 11, 2020

VIA EMAIL
Attorney General Gordon MacDonald
Office of the Attorney General
Consumer Protection Bureau
33 Capitol Street
Concord, NH 03301
Email: DOJ-CPB@doj.nh.gov

Re: Notice of Potential Data Security Incident

Dear Attorney General MacDonald:

We represent The Results Companies ("TRC"), a contact center customer service provider headquartered in Fort Lauderdale, Florida, in relation to a potential data security incident.

1. Nature of the matter.

On August 13, 2019, TRC discovered that an employee email account had been accessed without authorization. The unauthorized access was discovered when a fraudulent wire transfer involving solely TRC's corporate account was attempted. Upon discovery of the attempted fraudulent wire transfer, TRC immediately launched an investigation and determined that the employee email account had been used to facilitate the attempted fraudulent wire transfer. In the process of obtaining information to facilitate the attempted fraudulent wire transfer, it appears that the malicious actor may have accessed personal information without authorization. The information accessed may have included driver's license numbers and Social Security numbers. TRC is not aware of any fraudulent activity as a result of this matter.

2. Number of New Hampshire residents affected.

After a complex and detailed digital forensics investigation, on February 25, 2020, TRC learned that the personal information of five (5) residents of New Hampshire may have been accessed without authorization as a result of the matter. TRC will be notifying the potentially affected New Hampshire residents on or about March 11, 2020, via the attached consumer notification template. However, none of the persons to be notified were affected by the attempted fraudulent wire transfer because the transfer only involved TRC's corporate bank account. Out of an abundance of caution, TRC is offering twelve (12) months of complimentary credit monitoring and identity theft protection services to the potentially affected New Hampshire residents.

3. Steps taken relating to the matter.

After discovering the matter, TRC immediately hired a consulting firm who disabled all unauthorized access to the affected account. In addition, TRC engaged third party forensics firms to identify and eliminate any vulnerabilities and to increase the existing security of the email environment. TRC has also taken a number of actions to further enhance the existing security of its email environment and any personal information therein. These actions included implementation of the following additional security measures:

- Enabled multi-factor authentication;
- Restricted administrative access;
- Enhanced alerting on new account creation or privilege elevation;
- Enhanced event logging; and
- Disabled certain functions and blocked certain rules, such as auto-forwarding.

4. Contact information.

If you have any questions or need additional information, please contact me at 971.712.2795 or sean.hoar@lewisbrisbois.com.

Very truly yours,

Sean B. Hoar of
LEWIS BRISBOIS BISGAARD & SMITH LLP

Attachment: Template Consumer Notification Letter

C/O ID Experts
PO Box 4219
Everett WA 98204

ENDORSE

<<First Name>> <<Last Name>>
ADDRESS1
ADDRESS2
CSZ
COUNTRY

BREAK

SEQ
CODE 2D
Ver 1GE

To Enroll, Please Call:
1-833-554-0511
Or Visit:
https://ide.myidcare.com/trc
Enrollment Code: <<XXXXXXXX>>

March 6, 2020

RE: Notice of Potential Data Security Incident

Dear <<First Name>> <<Last Name>>,

This letter is to inform you of a potential data security incident that may have involved your personal information. At The Results Companies (TRC), we take the privacy and security of personal information very seriously. We therefore wanted to notify you of this matter, offer you complimentary identity protection services for 12 months, and provide you with steps you can take to protect your personal information.

What Happened: On August 13, 2019, TRC discovered that an employee email account had been accessed without authorization. The unauthorized access was discovered when a fraudulent wire transfer, involving solely TRC's corporate account, was attempted. Upon discovery of the attempted fraudulent wire transfer, TRC immediately launched an investigation and determined that the employee email account had been used to facilitate the attempted fraudulent wire transfer. As a precautionary measure, TRC engaged a digital forensics firm to assist with its investigation. The investigation revealed that in the process of obtaining information to facilitate the attempted fraudulent wire transfer, the malicious actor may have accessed personal information without authorization. On February 25, 2020, we determined that this matter may have involved your personal information.

What Information Was Involved: Information may have involved <<variable text>>.

What We Are Doing: As soon as we learned of this matter, we took the measures referenced above. We also implemented a number of measures to further enhance the existing security of our email platform in an attempt to prevent a similar occurrence in the future. We are also offering you identity protection services for 12 months at no charge to you.

What You Can Do: You can enroll in the identity protection services that we are offering for 12 months at no charge through ID Experts. We encourage you to contact ID Experts with any questions and to enroll in free MyIDCare services by calling 1-833-554-0511 or going to https://ide.myidcare.com/trc and using the Enrollment Code provided above. MyIDCare experts are available Monday through Friday from 9 am - 9 pm Eastern Time. Please note the deadline to enroll is June 5, 2020. You can also follow the recommendations included with this letter to protect your personal information.

For More Information: You will find detailed instructions for enrollment on the enclosed Recommended Steps document. Also, 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.

Please call 1-833-554-0511 or go to https://ide.myidcare.com/trc for assistance or for any additional questions you may have.

Sincerely,
The Results Companies

(Enclosure)

MyIDCare™

Recommended Steps to Help Protect Your Information

1. **Website and Enrollment.** Go to https://ide.myidcare.com/trc 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 MyIDCare 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, MyIDCare will be able to assist you.

3. Telephone. Contact MyIDCare at 1-833-554-0511 to gain additional information about this event 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 12 months 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 MyIDCare, notify them immediately by calling or by logging into the MyIDCare 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 the Attorney General.

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
1-866-349-5191
P.O. Box 105069
Atlanta, GA 30348-5069
www.equifax.com

Experian Fraud Reporting
1-888-397-3742
P.O. Box 9554
Allen, TX 75013
www.experian.com

TransUnion Fraud Reporting
1-800-680-7289
P.O. Box 2000
Chester, PA 19022-2000
www.transunion.com

It is necessary 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.

SEQ
CODE 2D

6. Security Freeze. By placing a security freeze, someone who fraudulently acquires your personal identifying information will not be able to use that information to open new accounts or borrow money in your name. You will need to contact 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 until 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 (http://www.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.

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

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.