LEWIS BRISBOIS

LEWIS BRISBOIS BISGAARD & SMITH LLP

Lindsay B. Nickle
2100 Ross Avenue, Suite 2000
Dallas, Texas 75201
Lindsay.Nickle@lewisbrisbois.com
Direct: 214.722.7141

February 20, 2020

File No. 6234.13860

VIA EMAIL

Attorney General Gordon MacDonald
Office of the Attorney General
New Hampshire Department of Justice
33 Capitol Street
Concord, NH 03301
Email: Doj.cpb@doj.nh.gov

Re: Notification of Data Security Incident

Dear Attorney General MacDonald:

I represent Insurance Recovery Group ("IRG"), headquartered in Westborough, Massachusetts, with respect to a recent data security incident described in greater detail below. IRG takes the protection of sensitive information very seriously and is taking steps to prevent similar incidents from occurring in the future.

1. **Nature of the Security Incident.**

On January 2, 2020, IRG discovered suspicious activity involving its email system. Upon discovering this incident, IRG launched an investigation and engaged a digital forensics firm to help determine what happened and what information may have been accessed. On January 17, 2020 the investigation determined that an unauthorized actor was able to access an IRG employee's user account and may have accessed or acquired emails containing personal information, including names, addresses, Social Security numbers, Dates of Birth, or Driver's Licenses. At this time, we are unaware of the misuse of any personal information as a result of this incident.

2. **Number of New Hampshire Residents Affected.**

IRG notified 137 residents of New Hampshire via first class U.S. mail on February 18, 2020. A sample copy of the notification letter sent to the affected individual is included with this correspondence.

3. **Steps Taken Relating to the Incident.**

IRG has taken steps in response to this incident to prevent similar incidents from occurring in the future. Those steps include working with leading cybersecurity experts to enhance the security of its email system.

4. **Contact Information.**

IRG remains dedicated to protecting the personal information in its control. If you have any questions or need additional information, please do not hesitate to contact me at (214) 722-7141 or via email at Lindsay.Nickle@lewisbrisbois.com.

Sincerely,

Lindsay B. Nickle of
LEWIS BRISBOIS BISGAARD & SMITH LLP

LBN:ls
Enclosure: Sample Consumer Notification Letter

Insurance Recovery Group

C/O ID Experts
10300 SW Greenburg Rd. Suite 570
Portland, OR, 97223

To Enroll, Please Call:
1-800-939-4170
Or Visit:
https://app.myidcare.com/account-creation/protect
Enrollment Code:
<<XXXXXXXX>>

<<First Name>> <<Last Name>>
<<Address1>> <<Address2>>
<<City>>, <<State>> <<Zip>>

February 18, 2020

Subject: Notice of Data Breach

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

We recently discovered a data security incident involving your personal information. At Insurance Recovery Group, we take the privacy and security of your information very seriously. This letter is intended to inform you about this incident and to provide you with information about steps that you can take to help protect your information, including offering you complimentary credit monitoring, identity monitoring and other services outlined below.

What Happened? On January 2, 2020, we discovered suspicious activity in our email system. Upon discovering this incident, we immediately launched an investigation and engaged a digital forensics firm to help us determine what happened and what information may have been accessed. We also reported the incident to the Federal Bureau of Investigation. We have found no evidence that your personal information has been misused.

Nonetheless, out of an abundance of caution, Insurance Recovery Group is notifying you of this incident and is providing you with information about steps that you can take to help protect your information.

What Information Was Involved? The information impacted may have included your name, address, Social Security number, Date of Birth, or Driver's License.

What Are We Doing? Insurance Recovery Group took the measures referenced above as soon as this incident was discovered. Additionally, we are providing you with information about the steps that you can take to help protect your personal information and, as an added precaution, we are offering you complimentary credit monitoring for one year through ID Experts. The ID Experts services include: credit monitoring, identity monitoring; $1 million in identity theft expense reimbursement insurance; and fraud prevention and resolution support.

What You Can Do: We recommend you activate your complimentary ID Experts services. Activation instructions and a description of the services being provided are included with this letter. To enroll, please visit **https://app.myidcare.com/account-creation/protect** or call **1-800-939-4170** and provide the following enrollment code: **<<XXXXXXXX>>**. Your 12 months of services will include the following:

SINGLE BUREAU CREDIT MONITORING: Monitoring of credit bureau for changes to the member's credit file such as new credit inquires, new accounts opened, delinquent payments, improvements in the member's credit report, bankruptcies, court judgments and tax liens, new addresses, new employers, and other activities that affect the member's credit record.

CYBERSCAN™: Dark Web monitoring of underground websites, chat rooms, and malware, 24/7, to identify trading or selling of personal information like SSNs, bank accounts, email addresses, medical ID numbers, driver's license numbers, passport numbers, credit and debit cards, phone numbers, and other unique identifiers.

IDENTITY THEFT INSURANCE: Identity theft insurance will reimburse members for expenses associated with restoring their identity should they become a victim of identity theft. If a member's identity is compromised, the policy provides coverage for up to $1,000,000, with no deductible, from an A.M. Best A-rated" carrier. Coverage is subject to the terms, limits, and exclusions of the policy.

FULLY-MANAGED IDENTITY RECOVERY: ID Experts' fully-managed recovery service provides restoration for identity theft issues such as (but not limited to): account creation, criminal identity theft, medical identity theft, account takeover, rental application, tax fraud, benefits fraud, and utility creation. This service includes a complete triage process for affected individuals who report suspicious activity, a personally assigned IDCare Specialist to fully manage restoration of each case, and expert guidance for those with questions about identity theft and protective measures.

To receive credit services, you must be over the age of 18, have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file. Additional information describing your services is included with this letter.

Please note you must enroll by May 18, 2020. If you have questions or need assistance, please call ID Experts at 1-800-939-4170.

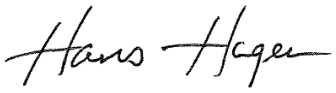
We also recommend that you:

- Close any potentially affected financial accounts;
- Review your account statements for discrepancies, and report any discrepancies to your bank;
- Place a fraud alert on your credit report; and
- Place a security freeze on your credit file.

For More Information: Further information about how to protect your personal information appears on the following page. If you have questions concerning this incident, please contact 1-800-939-4170, Monday-Friday (excluding holidays), 9 am to 8 pm Eastern Standard Time.

Please accept our sincere apologies and know that we deeply regret any worry or inconvenience that this may cause you.

Sincerely,



Hans A. Hagen
President & CEO
Insurance Recovery Group
200 Friberg Parkway, Suite 4000
Westborough, MA 01581

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 and review your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You should also 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 (the "FTC").

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 also contact one of the following three national credit reporting agencies:

Equifax	**Experian**	**TransUnion**	**Free Annual Report**
P.O. Box 105851	P.O. Box 9532	P.O. Box 1000	P.O. Box 105281
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19016	Atlanta, GA 30348
1-800-525-6285	1-888-397-3742	1-800-916-8800	1-877-322-8228
www.equifax.com	www.experian.com	www.transunion.com	www.annualcreditreport.com

Fraud Alert: You may want to consider placing a fraud alert 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. 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.

Security Freeze: Under U.S. law, you have the right to put a security freeze on your credit file for up to one year at no cost. This 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. 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.

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.

Federal Trade Commission	**Maryland Attorney General**	**North Carolina Attorney General**	**Rhode Island Attorney General**
600 Pennsylvania Ave, NW	200 St. Paul Place	9001 Mail Service Center	150 South Main Street
Washington, DC 20580	Baltimore, MD 21202	Raleigh, NC 27699	Providence, RI 02903
consumer.ftc.gov, and	oag.state.md.us	ncdoj.gov	http://www.riag.ri.gov
www.ftc.gov/idtheft	1-888-743-0023	1-877-566-7226	401-274-4400
1-877-438-4338			

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include knowing what is in your file; disputing incomplete or inaccurate information; and requiring consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, please visit https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf.