goulston&storrs
counsellors at law

Christian W. Habersaat
chabersaat@goulstonstorrs.com
(617) 574-3549 (tel)
(617) 574-4112 (fax)

September 27, 2018

Attorney General Gordon J. MacDonald
Office of the New Hampshire Attorney General
Attn: Security Breach Notification
33 Capitol Street
Concord, NH 03301

Re: Data Intensity - Data Breach Notification

Dear Attorney General MacDonald:

This firm represents Data Intensity. We are writing to notify you of a data security incident that potentially compromised the security of personal information of approximately five (5) New Hampshire residents who are employees or independent contractors of Data Intensity. Data Intensity's investigation into the event described below is ongoing, and this notice will be supplemented as any additional material information is learned.

Nature of Data Security Event

Data Intensity is a multi-cloud managed services provider focused on helping businesses manage their technologies and applications. The company, which maintains its global headquarters in Bedford, Massachusetts, apparently fell prey to a "phishing scam" that resulted in the potential exposure of data, including the personal information of New Hampshire residents, to an unauthorized party outside of Data Intensity.

On August 22, 2018, Data Intensity learned that an unauthorized party gained access to credentials of the company's Assistant Controller and used these credentials to enable email forwarding from the Assistant Controller's email mailbox to an outside email address. Upon learning of this event, Data Intensity immediately began an investigation, changed the password on the potentially compromised account and disabled the forwarding of emails from the Assistant Controller's mailbox. While Data Intensity has not yet confirmed the specific individual data that was or may have been accessed by an unauthorized party, the company understands that information contained in certain emails within the Assistant Controller's mailbox included such information as names, addresses, bank account and routing information of the company's New Hampshire employees and/or independent contractors. Company financial information was also likely accessed by an unauthorized party. Data Intensity believes from the

investigation undertaken to date that the email forwarding rule on the Assistant Controller's account was in place from July 9, 2018 to August 22, 2018.

Data Intensity engaged Mandiant, a leading cybersecurity firm, to further investigate the incident. Additionally, Data Intensity retained KL Discovery to conduct an analysis of the nature of the data potentially accessed by the unauthorized party. Data Intensity has also taken a series of remediation measures in response to the incident and has taken appropriate action to disable all automatic email forwarding capability enterprise wide.

Data Intensity is not aware of the misuse of the personal information that may have been accessed by an unauthorized party. Data Intensity will notify the employees whose information was the subject of the unauthorized access and that steps should be taken to be alert to signs of any misuse of their personal information. These employees will also be advised of their right to obtain a police report, how to request a security freeze and the ability to obtain credit reports from any of the credit reporting agencies. Data Intensity expects to provide written notice to the potentially affected individuals this week. A sample notification letter that Data Intensity will send to the affected employees and independent contractors is enclosed herewith. Additionally, Data Intensity will provide affected individuals with access to credit monitoring services for a period of twenty-four months at no charge.

Data Intensity will, as noted above, continue to investigate this incident with the assistance of its retained forensic and cybersecurity consultants, will monitor any inquiries from the persons potentially impacted, and will advise your office if any new significant information is learned.

We are, of course, available to discuss this matter with you, if you wish.

Very truly yours,

Christian W. Habersaat

CWH/vmm

Enclosure

DATA INTENSITY LETTERHEAD

Date

Employee Name
Address
City, MA

RE: Notice of Data Breach

Dear:

We are writing to notify you of an incident that may affect the security of your personal information. We are providing you with information regarding the incident, steps we have taken since discovering the incident, and what you can do to protect identity theft and fraud.

What Happened

On August 22, 2018 Data Intensity discovered the possibility that the unauthorized access of certain personal information, including yours, may have occurred as a result of a "phishing scam" into an email account of a Data Intensity employee.

What Information Was Involved

Our investigation determined that the impacted email account may have included names, addresses, and/or bank account, bank routing and other payroll-related information of Data Intensity employees and independent contractors.

What Data Intensity Is Doing to Address This Situation

Data Intensity takes the security and confidentiality of the personal information entrusted to us very seriously. While Data Intensity is not aware of and has not received any reports of the misuse of your personal information it has taken the appropriate steps to ensure that your sensitive information has been secured. Data Intensity is also conducting a thorough investigation into any unauthorized access of your personal information that may have occurred.

As a result of the potential unauthorized access of personal information, Data Intensity will provide you, if you wish, with access to identity monitoring services through *InfoArmor* at no charge. These services provide you with identity theft detection for twenty-four months from the date of enrollment.

To enroll in InfoArmor's comprehensive identity monitoring services at no charge to you, please visit **www.InfoArmor.com/ProtectDI** or call the InfoArmor's Privacy Advocate team at

1-800-289-2720 and mention that you are calling in connection with the Data Intensity incident. InforArmor's Privacy Advocates are available 24/7 to assist you and address any questions or concerns you may have.

What You Can Do to Address This Situation

You should remain vigilant for incidents of fraud and identity theft by regularly reviewing your account statements and monitoring free credit reports. If you discover any suspicious or unusual activity on your accounts or suspect fraud, be sure to report it immediately to your financial institutions. In addition, you may contact the Federal Trade Commission ("FTC"), law enforcement or the attorney general's office to report incidents of identity theft or to learn about steps you can take to protect yourself from identity theft. To learn more, you can go to the FTC's Web site, at www.consumer.gov/idtheft, or call the FTC, at (877) IDTHEFT (438-4338) or write to Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580.

For Maryland residents, the Attorney General can be reached at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-888-743-0023; or oag.state.md.us.

For North Carolina residents, the Attorney General can be contacted by mail at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226; or ncdoj.gov.

For Rhode Island residents, the Attorney General may be contacted at: 150 South Main St., Providence, RI 02903; 1-401-274-4400; or www.riag.ri.gov.

If you choose not to use the credit monitoring services provided by Data Intensity, but rather place a fraud alert on your own, you will need to contact one of the three major credit agencies directly at:

- **Experian (1-888-397-3742)**
- **Equifax (1-800-525-6285)**
- **TransUnion (1-800-680-7289)**

Also, should you wish to obtain a credit report and monitor it on your own:

- **IMMEDIATELY** obtain free copies of your credit report and monitor them upon receipt for any suspicious activity. You can obtain your free copies by going to the following website: www.annualcreditreport.com or by calling them toll-free at 1-877-322-8228. (Hearing impaired consumers can access their TDD service at 1-877-730-4204.)
- **Upon receipt of your credit report,** we recommend that you review it carefully for any suspicious activity.

For More Information

At Data Intensity we take our responsibilities to protect your personal information very seriously. We are deeply disturbed by this situation and apologize for any inconvenience it may

cause. If you have any questions or need further information regarding this incident, you may contact Sabrina Rothemeyer, Human Resources Director, at (781) 541-5900 x5937.

Sincerely,

Karl Stubelis
Chief Financial Officer