MULLEN COUGHLIN LLC
ATTORNEYS AT LAW

Christopher J. DiIenno
Office: (267) 930-4775
Fax: (267) 930-4771
Email: cdiienno@mullen.law

1275 Drummers Lane, Suite 302
Wayne, PA 19087

June 28, 2019

VIA U.S. MAIL

Attorney General Gordon J. MacDonald
Office of the New Hampshire Attorney General
Consumer Protection Bureau
33 Capitol Street
Concord, NH 03301

INTENDED FOR ADDRESSEE(S) ONLY

Re: Notice of Data Event

Dear Attorney General MacDonald:

We represent DataDirect Networks, Inc. ("DataDirect") located at 9351 Deering Avenue Chatsworth, California 91311. We are writing to notify your office of an incident that may affect the security of some personal information relating to one (1) New Hampshire resident. The investigation into this matter is ongoing, and this notice will be supplemented if any new significant facts are learned subsequent to its submission. By providing this notice, DataDirect does not waive any rights or defenses regarding the applicability of New Hampshire law, the applicability of the New Hampshire data event notification statute, or personal jurisdiction.

Nature of the Data Event

On or about April 18, 2019, DataDirect identified suspicious activity in an employee's email account. DataDirect immediately changed the employee's email password credentials and began an investigation into the incident. As part of the investigation, which is being conducted with the assistance of a leading third-party cyber security forensic expert, it was determined that an additional seven (7) DataDirect employees' email accounts were subject to intermittent unauthorized access from April 11, 2019 to May 21, 2019.

As part of the investigation, it was confirmed on June 18, 2019 that one of the affected employee's email accounts that was subject to unauthorized access contained personal information. The information that could have been subject to unauthorized access includes: name, address, and

Social Security number or tax identification number. The detailed review of the contents of all of affected employee email accounts is ongoing. If we identify additional personal information affecting New Hampshire residents was impacted, we will provide notice to those individuals and supplement this notice to you.

Notice to New Hampshire Resident

On or about June 28, 2019, DataDirect provided written notice of this incident to all known affected individuals, which includes one (1) New Hampshire resident. Written notice is being provided in substantially the same form as the letter attached here as ***Exhibit A***.

Other Steps Taken and To Be Taken

Upon discovering the event, DataDirect moved quickly to investigate and respond to the incident, assess the security of its systems, and notify potentially affected individuals. DataDirect is also working to implement additional safeguards and training to its employees. As part of these steps, DataDirect has already implemented multi-factor authentication for email access. Further, DataDirect is providing individuals whose personal information was potentially affected by this incident with access to one (1) year of credit monitoring services through TransUnion at no cost to the individuals.

Additionally, DataDirect is providing impacted individuals with guidance on how to better protect against identity theft and fraud, including advising individuals to report any suspected incidents of identity theft or fraud to their credit card company and/or bank. DataDirect is also providing individuals with information on how to place a fraud alert and security freeze on one's credit file, information on protecting against tax fraud, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud. DataDirect is providing notice of this incident to other state regulators as required.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4775.

Very truly yours,

Christopher J. DiIenno of
MULLEN COUGHLIN LLC

CJD:ncl
Enclosure

EXHIBIT A

DataDirect
NETWORKS

Return Mail Processing Center
PO Box 6336
Portland, OR 97228-6336

<<Name 1>>
<<Address 1>>
<<Address 2>>
<<City>><<State>><<Zip>>
<<Country>>

<<Date>>

RE: Notice of Data Breach

Dear <<Name 1>>:

DataDirect Networks, Inc. ("DataDirect") is writing to notify you of a recent data security incident that may impact some of your personal information. While we are unaware of any actual or attempted misuse of your personal information, we write to provide you with information about the incident, steps taken since discovering the incident, and what you can do to better protect against the potential misuse of your personal information, should you feel it is appropriate to do so.

What Happened? On or about April 18, 2019, DataDirect identified suspicious activity in an employee's email account. DataDirect immediately changed the employee's email password credentials and began an investigation into the incident. As part of the investigation, which is being conducted with the assistance of a leading third-party cyber security forensic expert, it was determined that a few DataDirect employees' email accounts were subject to intermittent unauthorized access from April 11, 2019 to May 21, 2019.

As part of the investigation, it was determined that an employee's email account that was subject to unauthorized access contained sensitive information related to you.

What Information Was Involved? The information in the email accounts that was subject to unauthorized access and related to you includes your name, <<Variable Data Text>>.

What We Are Doing. DataDirect takes the security of personal information in its care very seriously. DataDirect has engaged leading cyber security firms to assist our internal team with the forensic investigation and remediation efforts, and we have taken measures that are designed to remove the unauthorized access to our systems. DataDirect immediately changed passwords for the impacted accounts and, is working to implement additional security safeguards, including multi-factor authentication. DataDirect continues to monitor for signs of further activity or compromise. We are also providing resources, explained below, to help protect against potential misuse of your information.

As a safeguard, we have arranged for you to enroll, at no cost to you, in an online three-bureau credit monitoring service (*my*TrueIdentity) for one year provided by TransUnion Interactive, a subsidiary of TransUnion®, one of the three nationwide credit reporting companies.

To enroll in this service, go to the *my*TrueIdentity website at **www.mytrueidentity.com** and in the space referenced as "Enter Activation Code", enter the following unique 12-letter Activation Code **<<12-letter Activation Code>>** and follow the three steps to receive your credit monitoring service online within minutes.

If you do not have access to the Internet and wish to enroll in a similar offline, paper based, three-bureau credit monitoring service, via U.S. Mail delivery, please call the TransUnion Fraud Response Services toll-free hotline at **1-855-288-5422.** When prompted, enter the following 6-digit telephone pass code **697999** and follow the steps to enroll in the offline credit monitoring service, add an initial fraud alert to your credit file, or to speak to a TransUnion representative if you believe you may be a victim of identity theft.

You can sign up for the online or offline credit monitoring service anytime between now and **October 31, 2019**. Due to privacy laws, we cannot register you directly. Please note that credit monitoring services might not be available for individuals who do not have a credit file with TransUnion®, Experian® and Equifax®, or an address in the United States (or its territories) and a valid Social Security number. Enrolling in this service will not affect your credit score.

Once you are enrolled, you will be able to obtain one year of unlimited access to your TransUnion credit report and credit score. The daily three-bureau credit monitoring service will notify you if there are any critical changes to your credit files at TransUnion, Experian and Equifax, including fraud alerts, new inquiries, new accounts, new public records, late payments, change of address and more. The service also includes access to an identity restoration program that provides assistance in the event your identity is compromised to help you restore your identity and up to $1,000,000 in identity theft insurance with no deductible. (Policy limitations and exclusions may apply.)

What You Can Do. You can enroll to receive the free credit monitoring and identity restoration services being provided by DataDirect. You can also review the enclosed "Steps You Can Take to Protect Against Identity Theft and Fraud."

For More Information. We understand that you may have questions about this incident that may not be addressed in this letter. If you have additional questions, or need assistance, please call 877-848-4274, Monday through Friday, from 6:00 am to 6:00 pm Pacific Standard Time.

We sincerely apologize for this incident and regret any concern or inconvenience this may have caused you.

Sincerely,

Guy Colpitts

Guy Colpitts
General Counsel
DataDirect Networks, Inc.

Steps You Can Take to Protect Against Identity Theft and Fraud

The confidentiality, privacy and security of your personal information is one of our highest priorities. That's why we are sharing these steps you can take to protect your identity and uncover any fraudulent activity on your accounts.

We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity. Under U.S. law, you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report.

You have the right to place a "security freeze" on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security freeze is designed to prevent credit, loans and services from being approved in your name without your consent. However, you should be aware that using a security freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a security freeze on your credit report. Should you wish to place a security freeze, please contact the major consumer reporting agencies listed below:

Experian	**TransUnion**	**Equifax**
PO Box 9554	P.O. Box 2000	PO Box 105788
Allen, TX 75013	Chester, PA 19016	Atlanta, GA 30348-5788
1-888-397-3742	1-888-909-8872	1-800-685-1111
www.experian.com/freeze/center.html	www.transunion.com/credit-freeze	www.equifax.com/personal/credit-report-services

In order 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 (5) years, 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, a copy of either the police report, investigative report or complaint to a law enforcement agency concerning identity theft.

As an alternative to a security freeze, you have the right to place an initial or extended "fraud alert" on your file at no cost. An initial fraud alert is a one-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the agencies listed below:

Experian	**TransUnion**	**Equifax**
P.O. Box 2002	P.O. Box 2000	P.O. Box 105069
Allen, TX 75013	Chester, PA 19016	Atlanta, GA 30348
1-888-397-3742	1-800-680-7289	1-888-766-0008
www.experian.com/fraud/center.html	www.transunion.com/fraud-victim-resource/place-fraud-alert	www.equifax.com/personal/credit-report-services

You can further educate yourself regarding identity theft, fraud alerts, security freezes and the steps you can take to protect yourself by contacting the consumer reporting agencies, the Federal Trade Commission or your state Attorney General.

The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, D.C. 20580, www.identitytheft.gov, 1-877-ID-THEFT (1-877-438-4338); TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.

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