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

1275 Drummers Lane, Suite 302
Wayne, PA 19087

February 15, 2019

VIA U.S. MAIL

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

Re: Notice of Data Security Incident

Dear Mr. MacDonald:

Our firm represents Volt Information Sciences, Inc. ("Volt") and writes to inform your office of an incident that may affect the privacy of some personal information relating to two (2) New Hampshire residents. By providing this notice, Volt does not waive any rights or defenses regarding the applicability of New Hampshire law or personal jurisdiction.

Nature of the Data Event

On or around October 16, 2018, Volt determined that an unknown actor gained access to certain Volt employee email accounts and that some of the accounts were used to send out phishing emails. The employees' email credentials were changed, and the email accounts have been secured. A leading forensic investigation firm was retained to assist with Volt's investigation into what happened and what information may be affected. The investigation determined that the accounts at issue experienced unauthorized access between August 6, 2018 and October 4, 2018. The investigation also determined that the emails affected by this incident contained certain personal information.

The investigation determined that the following information related to New Hampshire residents was present in the emails affected by this incident: name and Social Security number

Notice to New Hampshire Residents

Since discovering this incident, Volt has been working diligently to confirm the nature and scope of the event, determine which individuals may have been affected, and determine contact information for those individuals.

On or around February 15, 2019, Volt will begin mailing written notice of this incident to potentially affected individuals, which includes two (2) New Hampshire residents. 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 unusual activity in an employees' email, Volt immediately took steps to investigate and respond to the incident, including changing the affected users' email credentials, and securing the email accounts. Volt has been working diligently, with the assistance of third party forensic investigators, to ensure the security of its email environment, determine the full nature and scope of the event, and identify potentially affected individuals. While Volt has measures in place to protect information in its systems, it is working to implement additional safeguards to protect the security of information.

Additionally, while to date, the investigation has found no evidence of actual or attempted misuse of personal information potentially affected by this event, in an abundance of caution, Volt is providing potentially impacted individuals with notice of this event. This notice includes an offer of access to credit monitoring and identity theft protection services for one (1) year through Kroll. Volt is also providing potentially impacted individuals with guidance on how to better protect against identity theft and fraud, including information on how to place a fraud alert and security freeze on one's credit file, 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 explanation of benefits form 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. Volt will also be providing notice of this event to other state regulators as required by law.

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 DiIenno of
MULLEN COUGHLIN LLC

CD/ajd
Enclosure

EXHIBIT A

VOLT

<<Date>> (Format: Month Day, Year)

<<FirstName>> <<MiddleName>> <<LastName>> <<NameSuffix>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip>>

RE: Notice of Data Breach

Dear <<FirstName>> <<LastName>>,

We write to inform you of a recent event that may affect the security of some of your personal information. While there is currently no evidence that your information has been misused, we are making you aware of the event, so you may take steps to better protect yourself against the possibility of identity theft or fraud, should you feel it necessary to do so.

What Happened?

On or around October 16, 2018, Volt Information Sciences ("Volt") confirmed that an unknown actor gained access to certain Volt employee email accounts and that some of the accounts were used to send out phishing emails. The employees' email credentials were changed, and the email accounts have been secured. A leading forensic investigation firm was retained to assist with Volt's investigation into what happened and what information may be affected. The investigation determined that the accounts at issue experienced unauthorized access between August 6, 2018 and October 4, 2018.

The contents of the accounts were reviewed through manual and programmatic processes to determine what sensitive data may have been accessed. On December 14, 2018, after the completion of the review, it was determined that the accounts may contain certain information related to you.

What Information Was Involved?

While we currently have no evidence that your information was subject to actual or attempted misuse, we have confirmed that your <<ClientDef1(data elements)>><<ClientDef2(data elements)>> were contained within the affected employee email accounts.

What We Are Doing.

The confidentiality, privacy, and security of information in our care is one of our highest priorities. Upon learning of this incident, we immediately took steps to secure the affected email accounts and to find out what happened. As part of our ongoing commitment to the security of the information in our care, we are reviewing our existing policies and procedures and also implementing additional technology tools and training to prevent or detect similar incidents from occurring in the future.

While we have no evidence of any actual or attempted misuse of any of the affected information, we have secured the services of Kroll to provide identity monitoring services at no cost to you for one year. More information on these services can be found in the enclosed "Steps You Can Take to Prevent Identity Theft and Fraud."

What You Can Do.

You may review the enclosed "Steps You Can Take to Prevent Identity Theft and Fraud" and take any action you think is appropriate for your specific situation. You may also enroll to receive the free identity monitoring services described above.

For More Information.

We understand you may have questions about this incident that are not addressed in this letter. To ensure your questions are answered in a timely manner, we have established a dedicated assistance line at 1-877-606-8501, Monday through Friday from 8:00 a.m. to 5:30 p.m. Central Time. You may also write to us at Attn: Legal Department, 2401 N. Glassell Street, Orange, CA 92865.

We take the privacy and security of the personal information that you entrusted to us very seriously. We sincerely regret any inconvenience or concern this incident may cause you.

Sincerely,

Linda Perneau
President and CEO
Volt Information Sciences

Steps You Can Take to Protect Against Identity Theft and Fraud

To help relieve concerns and restore confidence following this incident, we have secured the services of Kroll to provide identity monitoring at no cost to you for one year. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

Visit **krollbreach.idMonitoringService.com** to activate and take advantage of your identity monitoring services.

*You have until **May 15, 2019** to activate your identity monitoring services.*

Membership Number: <<Member ID>>

To receive credit services by mail instead of online, please call 1-877-606-8501. Additional information describing your services is included with this letter.

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
PO Box 9554
Allen, TX 75013
1-888-397-3742
www.experian.com/freeze/center.html

TransUnion
P.O. Box 2000
Chester, PA 19016
1-800-909-8872
www.transunion.com/credit-freeze

Equifax
PO Box 105788
Atlanta, GA 30348-5788
1-800-685-1111
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, provide 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, include 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 1-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
P.O. Box 2002
Allen, TX 75013
1-888-397-3742
www.experian.com/fraud/center.html

TransUnion
P.O. Box 2000
Chester, PA 19106
1-800-680-7289
www.transunion.com/fraud-victim-resource/place-fraud-alert

Equifax
P.O. Box 105069
Atlanta, GA 30348
1-888-766-0008
www.equifax.com/personal/credit-report-services

Although we have no reason to believe that your personal information has been used to file fraudulent tax returns, you can contact the IRS at www.irs.gov/Individuals/Identity-Protection for helpful information and guidance on steps you can take to address a fraudulent tax return filed in your name and what to do if you become the victim of such fraud. You can also visit www.irs.gov/uac/Taxpayer-Guide-to-Identity-Theft for more information.

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, DC 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 also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.

For North Carolina residents, the Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-566-7226 or 1-919-716-6400, www.ncdoj.gov.

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

For 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 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. We encourage you to 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.

Kroll.

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You've been provided with access to the following services[1] from Kroll:

Single Bureau Credit Monitoring. You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who can help you determine if it's an indicator of identity theft.

Fraud Consultation. You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration. If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator can dig deep to uncover the scope of the identity theft, and then work to resolve it.

[1] Kroll's activation website is only compatible with the current version or one version earlier of Internet Explorer, Chrome, Firefox, and Safari. To receive credit services, you must be over the age of 18 and 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.