NORTON ROSE FULBRIGHT

November 10, 2020

Via FedEx Overnight

Office of the Attorney General
Attn: Security Breach Notification
33 Capitol Street
Concord, NH 03301

Norton Rose Fulbright US LLP
799 9th Street NW
Suite 1000
Washington, DC 20001-4501
United States

Direct line +1 202 662 4691
chris.cwalina@nortonrosefulbright.com

Tel +1 202 662 0200
Fax +1 202 662 4643
nortonrosefulbright.com

Re: Legal Notice of Information Security Incident

Dear Sir or Madam:

We are writing on behalf of our client, Vecima Networks ("Vecima"), to notify your office that Vecima was the target of a ransomware attack that exposed the personal information of approximately one (1) New Hampshire residents.

On July 15, 2020, an unauthorized third party utilized compromised credentials of a Vecima user account to log onto Vecima's VPN. Subsequently on July 29, the third party logged onto Vecima's VPN using the credentials for the compromised account and leveraged the remote desktop protocol to access other systems and folders within Vecima's network.

On August 2, 2020, the unauthorized third party deployed the Maze ransomware in Vecima's systems which encrypted various files and systems stored on the compromised server. Vecima, through its legal counsel retained a forensic IT expert on August 6, 2020 who immediately conducted a forensic investigation into the incident. Subsequently, the organization paid a ransom to the unauthorized third party and in exchange the third party indicated they would not publically release any files the third party had purportedly accessed and that such files were deleted. The forensic investigation conducted by the external forensic IT expert was unable to confirm which specific files the unauthorized third party may have accessed.

Vecima has conducted a thorough review of the information that may have been accessed by the unauthorized third party and is now notifying the individuals whose personal data Vecima believes could have been exfiltrated. Vecima believes the following types of the New Hampshire residents' personal information may have been stolen: name, address, Social Security number, and banking information for payroll purposes.

We are not aware of any fraud or misuse of any personal information as a result of this incident. We do not believe personal information was targeted by the threat actor for identity theft purposes, but rather, such information may have been included in documents taken by the threat actor as part of the ransomware attack to extort the company.

Vecima continues to review its security measures, internal controls, and safeguards and continues to make changes to help prevent a similar incident from occurring in the future including but not limited to:

- Upgrading the firewall to eliminate the critical vulnerability;
- Updating old servers;
- Transferring the old domain to the Vecima corporate domain that includes stronger password requirements with more frequent changes; and
- Updating Antivirus software and verifying the installation on every server/computer.

We notified affected New Hampshire residents on November 9, 2020 and will be offering them 24 months of complimentary credit monitoring and fraud protection services. A copy of the notice letter is attached.

If you have any questions or need further information regarding this incident, please contact me at (202) 662-4691 or chris.cwalina@nortonrosefulbright.com.

Very truly yours,

Chris Cwalina

CGC/

Enclosure

VECIMA

[Date]

Dear [Name]:

Re: Notice of Data Incident

We take the privacy and security of our employees seriously and as a result, we are writing to inform you of a security Incident that may impact you. Your privacy is of the utmost importance to us, and we sincerely regret any concern this Incident may cause you.

What Happened

In August, Vecima was the victim of a ransomware attack by an unauthorized third party that resulted in the third party potentially accessing certain files from some of Vecima's servers and requested a ransom to delete the files (the **Incident**). Once Vecima discovered the Incident, we immediately conducted a detailed investigation and hired leading forensic IT experts to both contain and conduct a forensic investigation into the incident. After consulting with our forensic IT experts and legal counsel, Vecima payed the ransom and the unauthorized third party confirmed that it had deleted the files removed from Vecima's servers.

What Information Was Involved

While we currently have no evidence that your personal information was accessed by the third party, the following personal employee information is stored on our systems and may have been compromised: name, address, Social Security number, and banking information for payroll purposes. We have been advised by our forensic IT experts that the chance of misuse of the data by the third party is low, however out of an abundance of caution we chose to notify you of this Incident to advise you of the steps that are being taken to protect you and well as steps you can take to protect yourself.

What We Are Doing

To help protect your identity, we are providing you complimentary Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score/Cyber Monitoring services at no charge. These services provide you with alerts for twenty (24) months from the date of enrollment when changes occur to your Experian credit file. This notification is sent to you the same day that the change or update takes place with the bureau. Cyber monitoring will look out for your personal data on the dark web and alert you if your personally identifiable information is found online. Finally, we are providing you with proactive fraud assistance to help with any questions that you might have or in event that you become a victim of fraud, as well as a $1,000,000 insurance reimbursement policy.

To enroll in Credit Monitoring services at no charge, please log on to https://www.myidmanager.com and follow the instructions provided.

When prompted please provide the following unique code to receive services: <CODE HERE.>
In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter.

Please note that the service requires an internet connection and e-mail account and may not be available to minors under the age of 18 years of age. In addition, when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

For guidance with the CyberScout services CyberScout representatives are available for 90 days from the date of this letter between the hours of 8:00 am to 5:00 pm Eastern time, Monday through Friday. Please call the CyberScout help line 1-800-405-6108 and supply the fraud specialist with your unique code listed above. To extend these services, enrollment in the monitoring services described above is required.

VECIMA

What You Can Do

We recommend that you remain vigilant with respect to reviewing your account statements and credit reports and promptly report any suspicious activity or suspected identity theft to us and to the proper law enforcement authorities, including local law enforcement, your state's attorney general and/or the U.S. Federal Trade Commission ("FTC"). Please review the "Information About Identity Theft Protection" reference guide, enclosed here, which describes additional steps you may take to help protect yourself, including recommendations from the FTC regarding identity theft protection and details regarding placing a fraud alert or a security freeze on your credit file.

We additionally encourage you to be vigilant and to mitigate any potential harm by taking the following steps to protect yourself:

- change and create strong passwords for any online accounts, in particular those that use or relate to your social insurance number;
- be cautious of any unsolicited communications of whatever form (phone call, email, etc.) that ask for your personal information or refer you to a web page asking for personal information; and
- avoid clicking on links or downloading attachments from suspicious emails.

For More Information

Should you have any further questions or concerns regarding this incident or the protections available to you, you may contact the undersigned at 1-613-864-0054.

Sincerely,

Gerry Vreeswijk, Director, Human Resources

VECIMA

Information About Identity Theft Protection

Contact information for the three nationwide credit reporting companies is as follows:

Equifax	Experian	TransUnion
Phone: 800-685-1111 P.O. Box 740256 Atlanta, GA 30348 equifax.com	Phone: 888-397-3742 P.O. Box 9554 Allen, TX 75013 experian.com	Phone: 888-909-8872 P.O. Box 105281 Atlanta, GA 30348-5281 transunion.com

Free Credit Report. We remind you to be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit annualcreditreport.com or call toll free at 877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available from the U.S. Federal Trade Commission's (FTC) website at consumer.ftc.gov) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

For Colorado and Georgia residents:
You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit reporting agencies directly to obtain such additional report(s).

Security Freeze. Security freezes, also known as credit freezes, restrict access to your credit file, making it harder for identity thieves to open new accounts in your name. You can freeze and unfreeze your credit file for free. You also can get a free freeze for your children who are under 16. And if you are someone's guardian, conservator or have a valid power of attorney, you can get a free freeze for that person, too.

How will these freezes work? Contact all three of the nationwide credit reporting agencies Equifax, Experian, and TransUnion. If you request a freeze online or by phone, the agency must place the freeze within one business day. If you request a lift of the freeze, the agency must lift it within one hour. If you make your request by mail, the agency must place or lift the freeze within three business days after it gets your request. You also can lift the freeze temporarily without a fee.

Don't confuse freezes with locks. They work in a similar way, but locks may have monthly fees. If you want a free freeze guaranteed by federal law, then opt for a freeze, not a lock.

The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible and display your name, current mailing address and date of issue.

For Colorado and Illinois residents: You may obtain information from the credit reporting agencies and the FTC about security freezes.

Fraud Alerts. A fraud alert tells businesses that check your credit that they should check with you before opening a new account. As of Sept.18, 2018, when you place a fraud alert, it will last one year, instead of 90 days. Fraud alerts will still be free and identity theft victims can still get an extended fraud alert for seven years.

For Colorado and Illinois residents: You may obtain additional information from the credit reporting agencies and the FTC about fraud alerts.

VECIMA

FTC and State Attorneys General Offices. 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 FTC, or your state Attorney General. The FTC can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); TTY: 1-866-653-4261. The FTC 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.

For North Carolina residents: You may contact the North Carolina Office of the Attorney General, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, ncdoj.gov, 877-566-7226.

Obtaining a police report.
You have the right to obtain any police report filed in the United States in regard to this incident. If you are the victim of fraud or identity theft, you also have the right to file a police report.