goulston&storrs
counsellors at law

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

November 6, 2020

Office of New Hampshire Attorney General
Attn: Security Breach Notification
33 Capitol Street Concord, NH 03301
DOJ-CPB@doj.nh.gov

Re: New England Development - Data Breach Notification

Dear Sir/Madam:

This firm represents New England Development ("NED"). We are writing to notify you of a data security incident that *potentially* compromised the security of personal information of approximately one hundred and fifteen (115) New Hampshire residents who are current and former employees and independent contractors of NED. NED's investigation into the event described below is ongoing, and this notice will be supplemented, as is necessary, if any additional material information is learned.

Nature of Data Security Event

NED, a real estate development and management company that maintains its headquarters in Boston, Massachusetts, was the victim of a ransomware attack that resulted in the potential exposure of data, including possibly the personal information of New Hampshire residents, to an unauthorized party outside of NED.

In the early morning on October 3, 2020, NED discovered that it was the target of a ransomware attack. Immediately after discovering the incident, NED contacted Coretelligent, a provider of managed and co-managed IT, cybersecurity and cloud services, to begin incident response protocols, forensic investigation into the attack, and remediation and recovery efforts. Preliminary investigation revealed that the unknown attacker was on the network for approximately 10 hours before ransomware was executed, that the attacker was blocked from running malware on several servers, and that the attacker had logged off and was prevented from re-accessing the network by 11:40 PM on October 3rd. NED was able to restore its network from backup servers that were not affected by the attack, and decryption from the attacker was not required.

It was determined that the ransomware attack was from the *NetWalker* ransomware group. NED reported the incident to the FBI and is currently working with and is providing information

to the FBI relating to the attack. Although initial forensic investigation determined that NED's network was accessed by an unauthorized user, it was not determined whether any specific files or information had been exfiltrated. NED retained a second cybersecurity forensics firm, Arete Advisors, to communicate with the threat actor and to further investigate artifacts left following the attack. Through communications with the threat actor, on October 25, 2020, Arete Advisors confirmed that at least 16 files from NED's network appeared to have been exfiltrated. None of these files contained personally identifiable information ("PII"), and the investigation into the attack conducted to date has not determined whether PII was in fact accessed or acquired by the unauthorized actor.

While NED has not been able to determine that the unauthorized user accessed information containing PII, NED is reporting the incident in an abundance of caution and will notify individuals who may have had PII on NED's network about the attack and the possibility that their PII may have been accessed or acquired. NED will advise those individuals that steps should be taken to be alert to signs of any misuse of their personal information. These individuals will also be advised how to request a security freeze and the ability to obtain credit reports from any of the credit reporting agencies, and to remain vigilant by reviewing account statements and monitoring free credit reports. NED will offer each person complimentary credit monitoring services for a period of two (2) years. NED expects to provide written notice to the potentially affected individuals within a week. A sample notification letter that NED will send to the affected individuals is enclosed herewith.

NED will, as noted above, continue to investigate and monitor this incident with the assistance of its retained forensic consultant, 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

Enclosure

[NED Letterhead]

[Date]

[Individual Name]
[Street Address]
[City/State/Postal Code]

Dear [Individual Name]:

We are writing to notify you of an incident that *may* have impacted 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 October 3, 2020, New England Development ("NED") discovered that it was the target of a ransomware attack. Immediately after discovering the incident NED engaged providers of managed and co-managed IT, cybersecurity and cloud services, to begin incident response protocols and a thorough forensic investigation into the incident. NED also reported the incident to law enforcement.

What Information May Have Been Involved

While the investigation undertaken to date has determined that NED's network was accessed, it has not been determined whether any specific file containing your sensitive information was actually accessed or acquired by the unauthorized actor. In an abundance of caution, NED is notifying those individuals who may have been affected because of the types of information that were present on NED's network at the time of the attack including social security numbers.

What NED Is Doing To Address This Situation

NED takes the security and confidentiality of the personal information entrusted to us very seriously. While NED is not aware of and has not received any reports of the access or misuse of your personal information, it has taken the appropriate steps to ensure that your sensitive information has been secured. NED 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, NED will provide you, if you wish, with access to Single Bureau Credit Monitoring provided by *Kroll Information Assurance, LLC* at no charge for a period of two years.

How To Enroll For The Free Services

Visit **<<IDMonitoringURL>>** to activate and take advantage of your identity monitoring services.

You have until <<Date>> to activate your identity monitoring services.

Membership Number: **<<Member ID>>**

We have arranged a dedicated call center run by *Kroll* to assist with questions about how to protect your identity following this incident. You may call the *Kroll* service center at 1-800-xxx-xxxx, for further consultation. Please have your membership number ready.

What You Can Do To Address This Situation

You may consider placing a security freeze on your credit report. A security freeze prohibits a credit-reporting agency from releasing any information from a consumer's credit report without written authorization. However, please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing or other services.

To place a security freeze on your credit report, you must contact each of the three major consumer reporting agencies: Equifax (www.equifax.com); Experian (www.experian.com); and TransUnion (www.transunion.com):

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348
800-685-1111
www.equifax.com/personal/credit-report-services/credit-freeze

Experian Security Freeze
P.O. Box 9554 Allen, TX 75013
888-397-3742
www. Experian.com/freeze/center/html.

Trans Union
P.O. Box 160 Woodlyn, PA 19094
888-909-8872
www.transunion.com/credit-freeze

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.

The credit reporting agencies have one (1) business day after receiving your request by telephone or secure electronic means or three (3) business days after receiving your request by mail to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within five (5) business days and provide you with a unique personal identification number (PIN) or password, or both that can be used by you to authorize the removal or lifting of the security freeze.

To lift the security freeze in order to allow a specific entity or individual access to your credit report, you must call or send a written request to the credit reporting agencies by a secure electronic means or mail and include proper identification (name, address, and social security number) and the PIN number or password provided to you when you placed the security freeze as well as the identities of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have one (1) hour after receiving your request by telephone or secure electronic means or three (3) business days after receiving your request by mail to lift the security freeze for those identified entities or for the specified period of time.

Although NED is not aware of any reports of the access or misuse of your personal information we suggest that 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 identitytheft.gov, or call the FTC, at (877) IDTHEFT (877-438- 4338) or write to Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580.

Additional Information for Residents of the Following States:

For Connecticut residents, the Attorney General, can be contacted at 165 Capitol Avenue, Hartford, CT 06106, www.ct.gov/ag or by calling 860-808-5318.

For District of Columbia residents, the Attorney General can be contacted at 400 6th Street NW, Washington, D.C. 20001, https://oag.dc.gov/consumer-protection/consumer-alert-identity-theft, or by calling (202)727-3400.

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

For New York residents, the Attorney General can be contacted at The Capitol, Albany, NY 12224, https://ag.ny.gov/consumer-frauds/identity-theft or by calling 800-771-7755.

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

For Oregon residents, the Attorney General can be contacted at Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us or by calling 877-877-9392

For Rhode Island residents, the Attorney General can be contacted at Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, or by calling 401-274-4400

For More Information

NED takes its 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 Diane C. Retzky at (617) xxx-xxxx. Please recognize however that at this time we are unable to provide you with specific information as to the nature of the possible unauthorized access to your personal information.

Sincerely,

Diane C. Retzky