



Alyssa R. Watzman
1700 Lincoln Street, Suite 4000
Denver, Colorado 80203
Alyssa.Watzman@lewisbrisbois.com
Direct: 720.292.2052

July 16, 2021

VIA ELECTRONIC MAIL

Attorney General Gordon J. MacDonald
Office of the Attorney General
New Hampshire Department of Justice
33 Capitol Street
Concord, NH 03301
Email: attorneygeneral@doj.nh.gov

Re: Notice of Data Security Incident

To Whom It May Concern:

We represent Enfield Enterprises, Inc. (“Enfield”), a multi-faceted general construction firm headquartered in Springfield, Massachusetts. We are sending this letter, on behalf of Enfield, with respect to a data security incident recently discovered by Enfield that impacted personal information belonging to a New Hampshire resident. The impacted information may have included the resident’s Social Security number, driver’s license and/or other government identification number.

On June 6, 2021, Enfield discovered unusual activity within its network environment and immediately took steps to secure its systems. Enfield also began investigating the incident and engaged independent cybersecurity experts to assist with the investigation and remediation process. Enfield later learned that certain information was acquired without authorization as a result of the incident. On June 17, 2021, the investigation revealed that personal information belonging a New Hampshire resident was included in the affected data files. Enfield then worked diligently to identify the individuals and updated mailing addresses in order to provide notification of the incident

Enfield notified one (1) New Hampshire resident of this incident via the attached sample letter on July 13, 2021. Enfield also reported the incident to the Federal Bureau of Investigation and will provide whatever cooperation is needed to hold the perpetrators accountable. Enfield takes the security of all information within its possession very seriously.

July 16, 2021
Page 2

Please contact me should you have any questions.

Very truly yours,

/s/ Alyssa R. Watzman

Alyssa R. Watzman of
LEWIS BRISBOIS BISGAARD & SMITH LLP

Encl.: Sample Consumer Notification Letter

Enfield Enterprise Inc.
10300 SW Greenburg Rd. Suite 570
Portland, OR 97223



<<First Name>> <<Last Name>>
<<Address1>> <<Address2>>
<<City>>, <<State>> <<Zip>>

To Enroll, Please Call:
1-800-939-4170
Or Visit:
<https://app.idx.us/account-creation/protect>
Enrollment Code: <<XXXXXXXXXX>>

July 13, 2021

Re: Notice of Data Security Incident

Dear <<First Name>> <<Last Name>>,

We are writing to inform you of a recent data security incident experienced by Enfield Enterprises Inc. (“Enfield”) that may have impacted your personal information. Please read this letter carefully as it contains information regarding the incident, the type of information potentially involved, and the steps that you can take to help protect your personal information.

What Happened: On June 6, 2021, Enfield discovered that it had experienced a data security incident disrupting access to certain of its systems. In response, we took immediate steps to secure our systems and launched an investigation. We also engaged an independent digital forensics firm to assist with our recovery efforts, to determine what happened, and to identify any personal information that may have been accessed or acquired without authorization as a result of the incident. On June 17, 2021, we learned that files containing your personal information may have been acquired by an unauthorized third-party in connection with this incident, which is the reason for this notification. We are not aware of the misuse of any of the information contained in such files. Nevertheless, we are notifying you about this incident out of an abundance of caution and providing you with steps you can take to help protect your personal information.

What Information Was Involved: The information that may have been involved varied depending on the individual but may have included your name as well as your Social Security number, driver’s license or state/federal identification card number, passport number, and/or date of birth.

What We Are Doing: As soon as we learned of the incident, we took the steps described above. In addition, we implemented additional measures to enhance the security of our digital environment in an effort to minimize the likelihood of a similar event from occurring in the future. Furthermore, we reported the incident to the Federal Bureau of Investigation and are committed to assisting with its investigation into the matter.

We are also providing you with steps that you can take to help protect your personal information, and as an added precaution, we are offering you complimentary identity protection services through IDX, a data breach and recovery services expert. Your services include 24 months of credit monitoring¹ and dark web monitoring, a \$1,000,000 identity fraud loss reimbursement policy, and fully managed identity theft recovery services.

What You Can Do: Although we are not aware of any misuse of your information as a result of this incident, we encourage you to follow the recommendations on the following page to help protect your information. We also encourage you to enroll in the complimentary services being offered to you through IDX by visiting <https://app.idx.us/account-creation/protect>

¹ To receive credit monitoring 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.

creation/protect or by calling 1-800-939-4170 and using the Enrollment Code provided above. The deadline to enroll is October 13, 2021.

For More Information: If you have any questions regarding the incident or would like assistance with enrolling in the services offered, please contact IDX at 1-800-939-4170, Monday through Friday from 9 am to 9 pm Eastern Time (excluding holidays).

The security of your information is a top priority for Enfield. Please accept our sincere apologies and know that we deeply regret any worry or inconvenience that this may cause you.

Sincerely,

A handwritten signature in black ink, appearing to read 'D. Eastman', written in a cursive style.

Daniel Eastman, President
Enfield Enterprises Inc.

Steps You Can Take to Further Protect Your Information

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (FTC).

Copy of Credit Report: You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting <http://www.annualcreditreport.com/>, calling toll-free 1-877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can print this form at www.annualcreditreport.com/cra/requestformfinal.pdf. You also can contact one of the following three national credit reporting agencies:

Equifax

P.O. Box 105851
Atlanta, GA 30348
1-800-525-6285
www.equifax.com

Experian

P.O. Box 9532
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion

P.O. Box 1000
Chester, PA 19016
1-800-916-8800
www.transunion.com

Fraud Alert: You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least one year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at <http://www.annualcreditreport.com>.

Security Freeze: You have the right to put a security freeze on your credit file for up to one year at no cost. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security Number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC, or from your respective state Attorney General about fraud alerts, security freezes, and steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the Attorney General in your state.

Federal Trade Commission

600 Pennsylvania Ave, NW
Washington, DC 20580
consumer.ftc.gov, and
www.ftc.gov/idtheft
1-877-438-4338

Maryland Attorney General

200 St. Paul Place
Baltimore, MD 21202
oag.state.md.us
1-888-743-0023

New York Attorney General

Bureau of Internet and Technology
Resources
28 Liberty Street
New York, NY 10005
1-212-416-8433

North Carolina Attorney General

9001 Mail Service Center
Raleigh, NC 27699
ncdoj.gov
1-877-566-7226

Rhode Island Attorney General

150 South Main Street
Providence, RI 02903
<http://www.riag.ri.gov>
1-401-274-4400

Washington D.C. Attorney General

441 4th Street, NW
Washington, DC 20001
oag.dc.gov
1-202-727-3400

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include to know what is in your file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information; as well as other rights. For more information about the FCRA, and your rights pursuant to the FCRA, please visit http://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf.