



Allen E. Sattler
650 Town Center Drive, Suite 1400
Costa Mesa, California 92626
Allen.Sattler@lewisbrisbois.com
Direct: 714.668.5572

May 23, 2022

File No. 28310.1357

VIA EMAIL

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
ldtheft@oag.state.md.us

Re: Notification of Data Security Incident

Dear Maryland Office of the Attorney General:

Lewis Brisbois Bisgaard & Smith LLP represents C.R. England, Inc. in connection with a recent data security incident described in greater detail below. The purpose of this letter is to notify you of the incident in accordance with Maryland's data breach notification statute, Md. Code Ann. Comm. Law §§ 14-3501 *et seq.*

1. Nature of the Security Incident

On October 30, 2021, C.R. England discovered unauthorized activity within its computer network. When its IT department began troubleshooting to identify and fix the issue, it learned of the presence of an unauthorized party on certain systems within its network. Upon this discovery, C.R. England immediately began containment, mitigation, and remediation measures to reduce the impact on its operations. In addition, C.R. England engaged cybersecurity experts to supplement its response efforts, including conducting a forensic investigation to identify the source of the compromise.

The forensic investigation determined that an unknown third-party gained access to C.R. England's network and may have acquired certain data without authorization. Following this finding, C.R. England reviewed the affected files to determine whether they contain personal information relating to any individuals and if so, the categories of information involved for each.

On April 20, 2022, C.R. England determined that the affected files contained personal information relating to some of its employees. Upon this determination, C.R. England worked diligently to identify current address information for the affected individuals in order to provide notice of the incident. C.R. England completed this process for the majority of the affected individuals on May 17, 2022.

To date, there is no evidence to suggest that the information in the affected files was published, shared, or otherwise misused.

2. Number of Affected Maryland Residents & Information Involved

The incident involved personal information for approximately 1,782 Maryland residents. The information involved in the incident may differ depending on the individual but may include the following for affected Maryland residents: name, address, date of birth, Social Security number, and driver's license number. Again, C.R. England has no reason to believe that the information involved has been or will be published, shared, or otherwise misused.

3. Notification to Affected Individuals

On May 23-24, 2022, notification letters will be sent to affected Maryland residents by USPS First Class Mail. The notification letter provides resources and steps individuals can take to help protect their information. The notification letter also offers complimentary identity protection services, including credit monitoring, dark web monitoring, \$1 million identity fraud loss reimbursement policy, and fully-managed identity theft recovery services. A sample notification letter is enclosed.

4. Measures Taken to Address the Incident

In response to the incident, C.R. England retained cybersecurity experts and launched a forensics investigation to determine the source and scope of the compromise. C.R. England is in the process of implementing additional security measures to further harden its digital environment in an effort to prevent a similar event from occurring in the future.

In addition, C.R. England has reported the incident to the Federal Bureau of Investigation ("FBI") and will cooperate fully to assist with any investigation.

Finally, C.R. England is notifying the affected individuals and providing them with steps they can take to protect their personal information as discussed above and reporting the incident to nationwide consumer reporting agencies (*i.e.*, Equifax, Experian, and Transunion).

5. Contact Information

If you have any questions or need additional information regarding this incident, please do not hesitate to contact me at Allen.Sattler@lewisbrisbois.com or 714.668.5572.

Sincerely,



Allen E. Sattler of
LEWIS BRISBOIS BISGAARD & SMITH LLP

AES:JL

Encl.: Sample Consumer Notification Letter

cc: Jennifer Lee, Lewis Brisbois (jennifer.lee@lewisbrisbois.com)

Michael Ferragamo, Lewis Brisbois (Michael.Ferragamo@lewisbrisbois.com)



C.R. England
Return to IDX
P.O. Box 989728
West Sacramento, CA 95798-9728

TO ENROLL, PLEASE CALL:

1-833-909-0993

OR VISIT:

<https://response.idx.us/cr-england>

Enrollment Code: <<Enrollment>>

<<First Name>> <<Last Name>>

<<Address1>>

<<Address2>>

<<City>>, <<State>> <<Zip>>

May 23, 2022

RE: Notice of Data <<Variable Field 1>>.

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

I am writing to inform you of a recent data security incident experienced by C.R. England that may have involved 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 October 30, 2021, we discovered unauthorized activity on our systems. In response, we immediately began containment, mitigation, and restoration efforts to terminate the activity and to secure our network, systems, and data. In addition, we retained independent cybersecurity experts to conduct a forensic investigation into the incident and assist us in determining what happened.

The forensic investigation determined that there was unauthorized access to certain files stored within our systems. Based on these findings, we reviewed the affected files to identify the individuals whose personal information may have been impacted by this incident and the categories of information involved for each individual. On April 20, 2022, we determined that the affected files contained some of your personal information. We then worked diligently to identify current address information necessary to notify you of the incident. Please note that to date, **we have no reason to believe that your information was published, shared, or misused** as a result of this incident. Nevertheless, we are notifying you of the incident and providing resources to help protect your information.

What Information Was Involved: The information involved included the following data elements: your <<Variable Field 3>>.

What We Are Doing: After the steps described above, we implemented additional security measures to protect our digital environment and minimize the likelihood of future incidents. We also reported the incident to the Federal Bureau of Investigation and will cooperate to help identify and prosecute those responsible.

In addition, we are offering you <<12 or 24>> months of complimentary identity theft protection services through IDX, a data breach and identity recovery services expert. The identity protection services include credit monitoring, dark web monitoring, \$1 million identity theft reimbursement insurance, and fully managed identity recovery services at no cost to you. To receive these services, you must be over the age of 18 and have a Social Security number, an established credit file, and a residential address in the United States that is associated with your credit file.

What You Can Do: You can enroll in the complimentary identity protection services offered in this letter by calling 1-833-909-0993 or visiting <https://response.idx.us/cr-england> and using the Enrollment Code provided at the top of this letter. Please note that the deadline to enroll is August 23, 2022. You can also review the enclosed sheet that provides additional steps you can take to help protect your information.

For More Information: If you have any questions regarding the incident or would like assistance with enrolling in the identity protection services offered, please call 1-833-909-0993, Monday through Friday from 7:00 a.m. to 7:00 p.m. Mountain Time.

The privacy and security of your information is a top priority for C.R. England. We take this incident very seriously and we regret any worry or inconvenience this may cause you.

Sincerely,

Chad England, Chief Executive Officer
C.R. England

Steps You Can Take to Protect Your Personal 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 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 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 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
www.consumer.ftc.gov and
www.ftc.gov/idtheft
1-877-438-4338

Maryland Attorney General

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

New York Attorney General

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

North Carolina Attorney General

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

Rhode Island Attorney General

150 South Main Street
Providence, RI 02903
www.riag.ri.gov
1-401-274-4400

Washington D.C. Attorney General

441 4th Street, NW
Washington, DC 20001
www.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 https://files.consumerfinance.gov/f/documents/bcftp_consumer-rights-summary_2018-09.pdf.

