

Christine Czuprynski
Direct Dial: 248-220-1360
E-mail: cczuprynski@mcdonaldhopkins.com

October 12, 2020

VIA U.S. MAIL

Attorney General Gordon MacDonald
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

Re: California Eastern Laboratories, Inc. – Incident Notification

Dear Sir or Madam:

McDonald Hopkins PLC represents California Eastern Laboratories, Inc. (“CEL”). I am writing to provide notification of an incident at CEL that may affect the security of personal information of approximately three New Hampshire residents. CEL’s investigation is ongoing, and this notification will be supplemented with any new or significant facts or findings subsequent to this submission, if any. By providing this notice, CEL does not waive any rights or defenses regarding the applicability of New Hampshire law or personal jurisdiction.

On June 18, 2020, CEL became aware of a potential ransomware incident upon learning that malware had infected a number of CEL systems and encrypted files on several machines. Upon learning of the issue, CEL commenced an immediate and thorough investigation. As part of that investigation, CEL engaged external cybersecurity professionals experienced in handling these types of incidents. After an analysis of those files, CEL discovered on September 9, 2020 that certain elements of personal data were present in the encrypted files.

To date, CEL has no evidence that any of the information has been acquired by unauthorized persons or misused. Nevertheless, out of an abundance of caution, CEL wanted to inform you (and the affected residents) of the incident and to explain the steps it is taking to help safeguard the affected residents against identity fraud. CEL is providing the affected residents with written notification of this incident commencing on October 9, 2020 in substantially the same form as the letter attached hereto. CEL is providing the residents with 12 months of credit monitoring, and advising the residents about the process for placing a fraud alert and/or security freeze on their credit files and obtaining free credit reports. CEL is also providing the contact information for the consumer reporting agencies and the Federal Trade Commission.

At CEL, protecting the privacy of personal information is a top priority. CEL is committed to maintaining the privacy of personal information in its possession and has taken many precautions to safeguard it. CEL continually evaluates and modifies its practices to enhance the security and privacy of the personal information it maintains.

RECEIVED
OCT 16 2020
CONSUMER PROTECTION

October 12, 2020

Page 2

Should you have any questions concerning this notification, please contact me at (248) 220-1360 or cczuprynski@mcdonaldhopkins.com. Thank you for your cooperation.

Very truly yours,

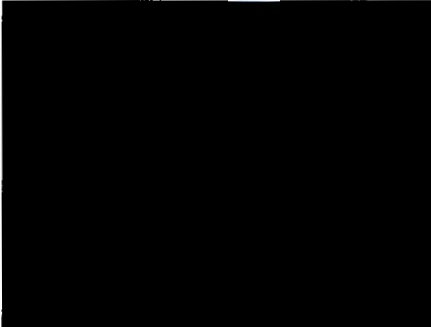
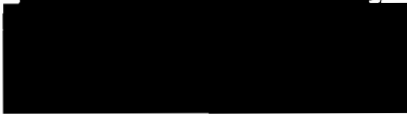
A handwritten signature in black ink, appearing to read "Christine Czuprynski". The signature is fluid and cursive, with the first name and last name clearly distinguishable.

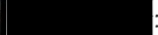
Christine Czuprynski

Encl.



California Eastern Laboratories, Inc.



Dear :

The privacy and security of the personal information we maintain is of the utmost importance to California Eastern Laboratories, Inc. (“CEL”). We are writing with important information regarding a recent security incident that may have impacted some of your information. We want to provide you with information about the incident, explain the services we are making available to you, and let you know that we continue to take significant measures to protect your information.

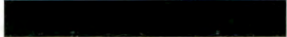
What Happened?

On June 18, 2020, we became aware of a potential ransomware incident which had infected a number of our systems and encrypted files on several machines. In addition to encrypting files, the unauthorized party may have removed a limited number of files and folders from our system.

What We Are Doing.

Upon learning of the issue, we commenced an immediate and thorough investigation. As part of our investigation, we engaged external cybersecurity professionals experienced in handling these types of incidents. The investigation worked to identify what personal information, if any, might have been present in those encrypted files. After an analysis of those files, we discovered on September 9, 2020 that certain elements of your personal data were present in the encrypted files. While we have no indication or evidence that any of that data has been or will be misused, we thought it important to notify you of this incident.

What Information Was Involved?

The impacted files contained some of your personal information, specifically your .

What You Can Do.

To protect you from potential misuse of your information, we are offering a complimentary one-year membership in Equifax® Credit Watch™ Gold. Equifax® Credit Watch™ Gold is completely free to you and enrolling in this program will not hurt your credit score. For more information on identity theft prevention and Equifax® Credit Watch™ Gold, including instructions on how to activate your complimentary one-year membership, please see the additional information provided in this letter.

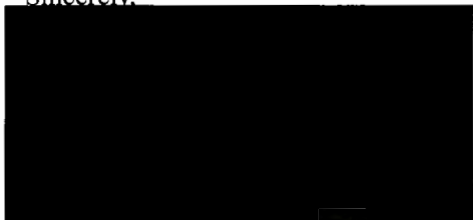
This letter also provides other precautionary measures you can take to protect your personal information, including placing a fraud alert and/or security freeze on your credit files, and/or obtaining a free credit report. Additionally, you should always remain vigilant in reviewing your account statements for fraudulent or irregular activity on a regular basis.

For More Information.

Please accept our sincere apologies that this incident occurred. We are committed to maintaining the privacy of personal information in our possession and have taken many precautions to safeguard it. We continually evaluate and modify our practices and internal controls to enhance the security and privacy of your personal information.

If you have any further questions regarding this incident, please call the dedicated and confidential toll-free response line that we have set up to respond to questions at [REDACTED]. This response line is staffed with professionals familiar with this incident and knowledgeable on what you can do to protect against misuse of your information. The response line is available [REDACTED].

Sincerely,



California Eastern Laboratories, Inc.

– OTHER IMPORTANT INFORMATION –

1. **Enrolling in Complimentary 12-Month Credit Monitoring.**

Activation Code: [REDACTED]

Equifax® Credit Watch™ Gold with 3-in-1 Credit Monitoring provides you with the following key features:

- 3-Bureau credit file monitoring¹ and alerts of key changes to your Equifax®, TransUnion®, and Experian® credit reports
- One Equifax 3-Bureau credit report
- Automatic Fraud Alerts² – With a fraud alert, potential lenders are encouraged to take extra steps to verify your ID before extending credit
- Wireless alerts (available online only) – Data charges may apply.
- Access to your Equifax® credit report
- Up to \$1 MM Identity Theft Insurance³
- Live agent Customer Service 7 days a week from 8 a.m. to 3 a.m.

Enrollment Instructions

To sign up online for online delivery go to [REDACTED]

1. **Welcome Page:** Enter the Activation Code provided above in the “Activation Code” box and click the “Submit” button.
2. **Register:** Complete the form with your contact information (name, gender, home address, date of birth, Social Security number and telephone number) and click the “Continue” button.
3. **Create Account:** Complete the form with your email address, create a Username and Password, review the Terms of Use and then check the box to accept and click the “Continue” button.
4. **Verify ID:** The system will then ask you up to four security questions to verify your identity. Please answer the questions and click the “Submit Order” button.
5. **Order Confirmation:** This page shows you your completed enrollment. Please click the “View My Product” button to access the product features.

To sign up for US Mail delivery, dial [REDACTED] for access to the Equifax Credit Watch Gold with 3-in-1 Credit Monitoring automated enrollment process. Note that all credit reports and alerts will be sent to you via US Mail only.

1. **Activation Code:** You will be asked to enter your Activation Code provided above.
2. **Customer Information:** You will be asked to enter your home telephone number, home address, name, date of birth and Social Security number.
3. **Permissible Purpose:** You will be asked to provide Equifax with your permission to access your credit file and to monitor your file. Without your agreement, Equifax cannot process your enrollment.
4. **Order Confirmation:** Equifax will provide a confirmation number with an explanation that you will receive your Fulfillment Kit via the US Mail (when Equifax is able to verify your identity) or a Customer Care letter with further instructions (if your identity can not be verified using the information provided). Please allow up to 10 business days to receive this information.

¹ Credit monitoring from Experian® and TransUnion® will take several days to begin.

² The Automatic Fraud Alert feature is made available to consumers by Equifax Information Services LLC and fulfilled on its behalf by Equifax Consumer Services LLC.

³ Identity theft insurance is underwritten by American Bankers Insurance Company of Florida or its affiliates. The description herein is a summary and intended for informational purposes only and does not include all terms, conditions and exclusions of the policies described. Please refer to the actual policies for terms, conditions and exclusions of coverage. Coverage may not be available in all jurisdictions.

Equifax® is a registered trademark of Equifax Inc. ©2017 Equifax Inc., Atlanta, Georgia. All rights reserved.

2. Placing a Fraud Alert on Your Credit File.

Whether or not you choose to use the complimentary 12-month credit monitoring services, we recommend that you place an initial 1-year “fraud alert” on your credit files, at no charge. A fraud alert tells creditors to contact you personally before they open any new accounts. To place a fraud alert, call any one of the three major credit bureaus at the numbers listed below. As soon as one credit bureau confirms your fraud alert, they will notify the others.

Equifax

P.O. Box 105069
Atlanta, GA 30348
www.equifax.com
1-800-525-6285

Experian

P.O. Box 2002
Allen, TX 75013
www.experian.com
1-888-397-3742

TransUnion LLC

P.O. Box 2000
Chester, PA 19016
www.transunion.com
1-800-680-7289

3. Placing a Security Freeze on Your Credit File.

If you are very concerned about becoming a victim of fraud or identity theft, you may request a “security freeze” be placed on your credit file, *at no charge*. A security freeze prohibits, with certain specific exceptions, the consumer reporting agencies from releasing your credit report or any information from it without your express authorization. You may place a security freeze on your credit report by sending a request in writing or by mail, to all three nationwide credit reporting companies. To find out more about how to place a security freeze, you can use the following contact information:

Equifax Security Freeze

P.O. Box 105788
Atlanta, GA 30348
<https://www.freeze.equifax.com>
1-800-685-1111

Experian Security Freeze

P.O. Box 9554
Allen, TX 75013
<http://experian.com/freeze>
1-888-397-3742

TransUnion Security Freeze

P.O. Box 2000
Chester, PA 19016
[http://www.transunion.com/
securityfreeze](http://www.transunion.com/securityfreeze)
1-888-909-8872

In order to place the security freeze, you’ll need to supply your name, address, date of birth, Social Security number and other personal information. After receiving your freeze request, each credit monitoring company will send you a confirmation letter containing a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

If you do place a security freeze *prior* to enrolling in the credit monitoring service as described above, you will need to remove the freeze in order to sign up for the credit monitoring service. After you sign up for the credit monitoring service, you may refreeze your credit file.

4. Obtaining a Free Credit Report.

Under federal law, you are entitled to one free credit report every 12 months from each of the above three major nationwide credit reporting companies. Call **1-877-322-8228** or request your free credit reports online at **www.annualcreditreport.com**. Once you receive your credit reports, review them for discrepancies. Identify any accounts you did not open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting company.

5. Additional Helpful Resources.

Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Checking your credit report periodically can help you spot problems and address them quickly.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call your local law enforcement agency and file a police report. Be sure to obtain a copy of the police report, as many creditors will want the information it contains to absolve you of the fraudulent debts. You may also file a complaint with the FTC by contacting them on the web at www.ftc.gov/idtheft, by phone at 1-877-IDTHEFT (1-877-438-4338), or by mail at Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580. Your complaint will be added to the FTC’s Identity Theft Data Clearinghouse, where it will be accessible to law enforcement for their investigations. In addition, you may obtain information from the FTC about fraud alerts and security freezes.

If this notice letter states that your financial account information and/or credit or debit card information was impacted, we recommend that you contact your financial institution(s) to inquire about steps to take to protect your account(s), including whether you should close your account(s) or obtain a new account number(s).