

RECEIVED

JUL 21 2021

CONSUMER PROTECTION

July 19, 2021

Attorney General John Formella
NH Department of Justice
33 Capitol Street
Concord, NH 03301

Dear Attorney General Formella:

Pursuant to the requirements of NH Rev. Stat. § 359-C:20(I)(b), we are writing to notify you of a data security incident involving five (5) New Hampshire residents whose social security numbers may have been accessed by an unauthorized third party.

Massachusetts Continuing Legal Education ("MCLE") is a 501(c)(3) non-profit organization that provides continuing legal education courses for legal professionals. Although MCLE contracts with outside vendors to provide payroll services, process credit card payments, and manage employee benefits, the MCLE server does contain a small number of files that contain the personal identifying information ("PII") of individuals who reside in a number of different states, including New Hampshire.

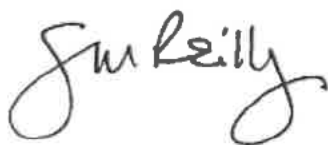
Starting approximately March 20, 2021, MCLE was subjected to a ransomware attack, and MCLE's computer systems were accessed and encrypted by an unidentified and unauthorized third party. MCLE learned of the attack on March 20, 2021, when ransomware activated on its local area network and caused the MCLE's public website to go down. Without paying a ransom, MCLE was able to restore its systems and clear them of any malicious files. However, it was subsequently discovered that, while they had control of MCLE's systems, the third party had the ability to access PII including social security numbers, driver's license numbers and credit card numbers in electronic form. MCLE does not know the identity of the person(s) responsible for the breach, whether there was any foreign country involvement, or the cause of the breach. MCLE is unaware of any resulting identity theft, fraud or financial losses to consumers.

Upon learning of the issue, MCLE promptly secured the assistance of its legal team, reported this wrongdoing to outside law enforcement using the Internet Crime Complaint Center, and retained forensic experts to regain access to MCLE's servers, assess the scope of the hackers' access to MCLE's systems and data, and identify and implement remedial measures to prevent future compromises to the security of the PII that MCLE maintains. For example, MCLE and its experts have forensically assessed infected server restores, reset admin and user passwords, disabled some accounts, monitored processes and services, enabled multi-factor authentication, commenced an exhaustive cybersecurity assessment. In addition, MCLE is implementing additional security awareness training for staff and installing an early warning detection and response system.

As more fully described in the attached template of the written notice of the incident that MCLE is sending to the five affected residents of New Hampshire on or about July 21, 2021, MCLE is offering the affected individuals 24 months of identity-theft protection and credit monitoring through Experian free of charge.

Should you have any questions, please contact Sal Ricciardone, MCLE's Director of Philanthropy & Special Projects, by phone at 617-896-1596 or by email at sricciardone@mcle.org.

Sincerely,

A handwritten signature in black ink, reading "John M. Reilly". The signature is written in a cursive, flowing style with a large initial "J" and "M".

John M. (Jack) Reilly
MCLE Executive Director

**NOTICE OF DATA BREACH
IMPORTANT - PLEASE READ THIS ENTIRE LETTER**

July 21, 2021

«First_Name» «Last_Name»
«AddressBlock»

«GreetingLine»

I am writing to inform you of a data security breach in which some of your personally identifiable information ("PII") may have been affected and to share with you important information about protecting your PII.

What happened?

Starting approximately March 20, 2021, Massachusetts Continuing Legal Education ("MCLE") was subjected to a ransomware attack, and MCLE's computer systems were accessed and encrypted by an unidentified and unauthorized third party. Without paying a ransom, MCLE was able to restore its systems and clear them of any malicious files. However, while they had control of MCLE's systems, the third party had the ability to access certain data including your social security number. We do not know if your PII actually was accessed.

What information was involved?

MCLE has determined that PII consisting of social security numbers, driver's license numbers and credit card numbers were impacted by this breach. In your particular case, the third party had the ability to access your social security number.

What are we doing?

Upon learning of the issue, MCLE promptly secured the assistance of our legal team, reported this wrongdoing to outside law enforcement using the Internet Crime Complaint Center, and retained forensic experts to regain access to MCLE's servers, assess the scope of the third party's access to MCLE's systems and data, and identify and implement remedial measures to prevent future compromises to the security of the PII that MCLE maintains. For example, MCLE and its experts have forensically assessed infected server restores, reset admin and user passwords, disabled some accounts, monitored processes and services, enabled multi-factor authentication, and commenced an exhaustive cybersecurity assessment. In addition, MCLE is implementing additional security awareness training for staff and installing an early warning detection and response system.

What we are doing to protect your information:

To help protect your identity, we are offering a complimentary 24-month membership of Experian's® IdentityWorksSM. This product provides you with superior identity detection and resolution of identity theft, if needed. To activate your membership and start monitoring your personal information please follow the steps below:

- Ensure that you **enroll by:** October 31, 2021 (Your code will not work after this date.)

- **Visit** the Experian IdentityWorks website to enroll: <https://www.experianidworks.com/credit>
- Provide your **activation code**: «**Activation_Codes**»

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 877-890-9332 by October 31, 2021. Be prepared to provide engagement number [REDACTED] as proof of eligibility for the identity restoration services by Experian.

Additional details regarding your 24-month Experian IdentityWorks Membership:

A credit card is **not** required for enrollment in Experian IdentityWorks.

You can contact Experian immediately regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.
- **Credit Monitoring:** Actively monitors Experian file for indicators of fraud.
- **Identity Restoration:** Identity Restoration agents are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **Up to \$1 Million Identity Theft Insurance:** Provides coverage for certain costs and unauthorized electronic fund transfers.

If you believe there was fraudulent use of your information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent at 877-890-9332. If, after discussing your situation with an agent, it is determined that Identity Restoration support is needed, then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that this identity restoration support, if needed, is available to you for 24 months from the date of this letter in accordance with the terms we describe herein. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration. You will also find self-help tips and information about identity protection at this site.

What you can do.

We suggest that you to take the following steps to mitigate possible misuse of your personal information:

1. Sign up for IdentityWorks protection in accordance with the instructions above. This service will be provided **FREE OF CHARGE** to you for 24 months.
2. Place a fraud alert on your credit report (see below for details).
3. Remain vigilant by reviewing records of your personal account and monitoring your credit reports.
4. Place a security freeze on your credit report (see below for details).

RESOURCES AND SUGGESTIONS:

Credit Report Fraud Alert

You may place a fraud alert on your credit report, which may help prevent someone from opening accounts in your name or changing your existing accounts. You may contact any one of the three major credit bureaus listed below to do so. When one credit bureau confirms your fraud alert, the others will be notified automatically of the alert.

Equifax
P.O. Box 740256
Atlanta, GA 30374
800-766-0008
www.equifax.com

Experian
P.O. Box 4500
Allen, TX 75013
888-397-3742
www.experian.com

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

Equifax: https://www.alerts.equifax.com/AutoFraud_Online/jsp/fraudAlert.jsp.

Experian: <https://www.experian.com/corporate/personal-services-contacts.html>

You may also order a credit report. You are entitled to receive a free credit report annually from each of the three credit bureaus listed above.

Credit Report Security Freeze

You may place a security freeze on your credit reports, which would prohibit a credit reporting agency from releasing any information from your credit report without your written permission. You should be aware, however, 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. A credit reporting agency may charge you fees for placing, removing, and replacing a security freeze. The fees vary from state to state and depend on your circumstances. If you are an identity theft victim with a valid police report, a credit reporting agency may provide you with security freeze services free of charge.

Other

- Remain vigilant in reviewing your account statements and monitoring free credit reports to protect yourself against fraud and identity theft.
- You may obtain additional information about how to avoid identify theft from

Federal Trade Commission¹
Consumer Response Center
Washington, DC 20580
Toll Free helpline: 1-877-ID-THEFT (1-877-438-4338)
TTY 1-866-653-4261
<http://www.ftc.gov/>

- If you suspect that someone has stolen or misused your personal information or that you are a victim of identity theft, you should immediately report the incident to local law enforcement or the attorney general for the state in which you reside.

For more information.

Do not hesitate to contact Sal Ricciardone, MCLE's Director of Philanthropy & Special Projects, by phone at 617-896-1596 or by email at sricciardone@mcle.org if you have any questions or concerns about this incident. If you prefer to use a toll-free number, please leave a message for Sal Ricciardone at 1-800-966-6253. Your call will be returned promptly.

We sincerely apologize for this incident. We know you trust us to protect your information when you share it with us, and we want to assure you that we consistently strive to take reasonable measures to do so.

Sincerely,



John M. (Jack) Reilly
Executive Director

¹ If you are a resident of North Carolina, additional information is available by contacting the North Carolina Attorney General's Office, 114 West Edenton Street, Raleigh, NC 27603, Tel: 1-919-716-6400, <http://www.ncdoj.gov>. Residents of Maryland may contact the Maryland Attorney General, 200 St. Paul Place, 25th Floor, Baltimore, MD 21202, Tel: 1-410-576-6566, <http://www.marylandattorneygeneral.gov>. Residents of the District of Columbia may contact the D.C. Attorney General, 400 6th Street, NW, Washington, DC 20001, Tel: 1-202-727-3400, <http://www.oag.dc.gov>.