



Kamran Salour
650 Town Center Drive, Suite 1400
Costa Mesa, CA 92626
kamran.salour@lewisbrisbois.com
Direct: 714.966.3184

October 3, 2024

VIA EMAIL

Attorney General Anthony G. Brown
Office of the Attorney General
200 St. Paul Place
Baltimore, MD 21202

Email: IDTheft@oag.state.md.us

Re: Notification of Data Security Incident

To Whom It May Concern:

Lewis Brisbois represents Judge Rotenberg Educational Center (“JRC”) located in Canton, Massachusetts, 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 data breach notification law.

1. Nature of the Security Incident

On February 13, 2024, JRC discovered that it had fallen victim to a ransomware attack. JRC promptly engaged a team of cybersecurity experts to assist it with conducting a forensic investigation to determine whether any data or personal information was impacted by the incident. On March 25, 2024, the investigation determined that certain data was impacted by the incident. JRC then began a review of the data to determine whether any personal information belonging to individuals was accessed or acquired without authorization as a result of this incident. On September 5, 2024, JRC determined that personal information was affected by the incident and moved to identify addresses for the impacted individuals in order to notify them of the incident. On September 25, 2024, JRC identified current addresses and moved to notify individuals of the incident.

2. Type of Information and Number of Maryland Residents Affected

JRC notified nine (9) residents of Maryland of this data security incident via first class U.S. mail on October 3, 2024. The information accessed and acquired by the unauthorized actor responsible for this incident included name, Social Security number, and/or driver’s license or state identification

card number. A sample copy of the notification letter sent to these individuals is included with this correspondence.

3. Steps Taken Relating to the Incident

JRC reported the incident to the FBI and will provide whatever cooperation is necessary to hold the perpetrators accountable. JRC has also implemented additional security features in an effort to prevent a similar incident from occurring in the future. Further, JRC has offered all individuals whose information was involved twelve (12) months of complimentary services through TransUnion, which includes credit monitoring, cyber monitoring, identity theft restoration services, an insurance reimbursement policy, and access to a call center.

4. Contact Information

JRC remains dedicated to protecting the personal information in its possession. If you have any questions or need additional information, please do not hesitate to contact me at (714) 966-3184 or by email at Kamran.Salour@lewisbrisbois.com.

Regards,

A handwritten signature in black ink, appearing to read 'Kam Salour', with a stylized flourish at the end.

Kamran Salour of
LEWIS BRISBOIS BISGAARD & SMITH LLP

Encl.: Sample Consumer Notification Letter

Judge Rotenberg Educational Center, Inc.
c/o Cyberscout
PO Box 1286
Dearborn, MI 48120-9998


Judge Rotenberg Educational Center
250 Turnpike Street
Canton, MA 02021



October 3, 2024

Re: Notice of Data Security Incident

Dear ,

Judge Rotenberg Educational Center (“JRC”) is writing to notify you of a recent data security incident that involved your personal information. This letter informs you of this incident and the steps you can take to help protect your personal information and offers you complimentary credit monitoring and identity protection services.

What Happened? On February 13, 2024, JRC discovered that it had fallen victim to a ransomware attack. JRC promptly engaged a team of cybersecurity experts to assist it with conducting a forensic investigation to determine whether any data or personal information was impacted by the incident. On March 25, 2024, the investigation determined that certain data was impacted by the incident. JRC then began a review of the data to determine whether any personal information belonging to individuals was accessed or acquired without authorization as a result of this incident. On September 5, 2024, JRC determined that personal information was affected and moved to identify addresses for the impacted individuals in order to notify them of the incident. On September 25, 2024, JRC identified current addresses and moved to notify individuals.

What Information Was Involved? The impacted information included your name, .

What Are We Doing? As soon as JRC discovered the incident, it took the steps described above. JRC also reported the incident to federal law enforcement, and will provide whatever cooperation is necessary to hold the perpetrators accountable. JRC implemented additional security measures to minimize the risk of a similar incident occurring in the future.

To help relieve concerns following this incident, JRC is offering you access to **Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score** services at no charge. These services provide you with alerts for  months from the date of enrollment when changes occur to your credit file. This alert is sent to you the same day that a change or update takes place with the bureau. Finally, JRC is providing you with proactive assistance to help with any questions that you might have or in the event that you become a victim of fraud. These services will be provided by Cyberscout, a TransUnion company specializing in fraud assistance and remediation services.

What Can You Do? JRC recommends that you review the guidance included with this letter about how to protect your personal information. In addition, JRC recommends enrolling in the complimentary services being offered by Cyberscout, a TransUnion company, to further protect your personal information. To receive credit monitoring services, you must be over the age of eighteen (18) and have established credit in the U.S., have a Social Security number to your name, and have a U.S. residential address associated with your credit file.

0000102G0500

P

To enroll in the complimentary credit monitoring and identity protection services, please log on to <https://bfs.cyberscout.com/activate> and follow the instructions provided. When prompted please provide the following unique code to receive the services: [REDACTED]

In order for you to receive the credit monitoring and identity protection services, the enrollment deadline is December 25, 2024. The enrollment requires an internet connection and e-mail account and may not be available to minors under the age of eighteen (18) years of age. Please note that when signing up for identity protection services, you may be asked to verify personal information for your own protection to confirm your identity.

Upon completion of the enrollment process, you will have access to the following features:

- Access to a credit report with credit score.
- Credit monitoring alerts with email notifications to key changes on a consumer's credit file.
- Identity theft insurance of up to \$1,000,000 in coverage to protect against potential damages related to identity theft and fraud.
- Assistance with reading and interpreting credit reports for any possible fraud indicators.
- Assistance with answering any questions individuals may have about fraud.

For More Information. If you have any questions regarding the incident or would like assistance with enrolling in the services offered, please call 1-844-428-0742 between 8:00 A.M. ET to 8:00 P.M. ET, Monday through Friday, excluding holidays.

JRC appreciates your understanding and deeply regrets any worry or inconvenience that this may cause you.

Sincerely,

Judge Rotenberg Educational Center

STEPS YOU CAN TAKE TO HELP 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 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

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

Maryland Attorney General
200 St. Paul Place
Baltimore, MD 21202
www.marylandattorneygeneral.gov
1-888-743-0023

Rhode Island Attorney General
150 South Main Street
Providence, RI 02903
www.riag.ri.gov
1-401-274-4400
The total number of Rhode Island residents receiving notification of this incident is 997.

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

**Washington D.C. Attorney
General**
441 4th Street, NW
Washington, DC
20001 oag.dc.gov
1-202-727-3400



00001020280000

P

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://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf>.