KIRKLAND & ELLIS

<<Date>> (Format: Month Day, Year)

Parent or Guardian of
<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country>>

NOTICE OF DATA BREACH

Dear **Parent or Guardian of** <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

We are writing to notify you of an issue that involves certain of your student's personal information, which we needed to review in connection with our representation of Illuminate Education, Inc. ("Illuminate") in certain legal matters regarding a January 2022 data security incident at Illuminate. Illuminate is an education company that provides applications and technology support to schools and school districts.

What Happened?

On May 31, 2023, we were informed by our third-party software provider, Progress Software, of a global cybersecurity issue involving its MOVEit Transfer solution. MOVEit is a file transfer tool used by governments, companies, and organizations worldwide, many of whom were impacted by this global cybersecurity incident. According to Progress Software, unauthorized actors discovered a previously unknown cybersecurity vulnerability in the MOVEit Transfer software that could be exploited to gain unauthorized access to files being transferred using the tool. After learning of the issue, we quickly initiated an investigation and took steps to secure our MOVEit repository. Through our investigation, we found that, between approximately May 27 and May 31, 2023, an unauthorized third party obtained certain of our files that we transferred through the MOVEit tool.

What Information Was Involved?

We have been working diligently to review the involved files to understand their nature and scope. Based on this review, we recently concluded that certain of the involved files may have included one or more of the following categories of personal information: student name, academic and behavior information, enrollment information, accommodation information, special education information, student disability code and description, date of birth, student identification number, and student demographic information. The types of student information involved varied by individual. We can confirm that the data involved did not contain Social Security numbers, credit card numbers, or bank account numbers.

What We Are Doing

We have been working diligently with leading cybersecurity experts to determine the nature and scope of how the MOVEit cybersecurity issue affected our MOVEIt repository. We also reported and continue to communicate with law enforcement about the issue.

What You Can Do

We regret any inconvenience this may cause you and are informing you about this issue so you can take steps to help protect your student's information. Steps you can take include:

- Register for Identity Monitoring Services. We have arranged to offer you certain identity monitoring services for your student for one year at no cost to you.
- Remain Vigilant. We encourage you to remain alert for any unsolicited communications regarding your student's personal information, review account statements associated with your student for suspicious activity, and monitor free credit reports, if available.

- Review the Enclosed Reference Guide. The enclosed Reference Guide provides information on registration for the identity protection services and recommendations on the protection of personal information.

For More Information

If you have any questions regarding this issue, please call **[insert call center toll-free number], Monday through Friday from 8:00 a.m. to 5:30 p.m. Central Time, excluding major U.S. holidays**.

Sincerely,

[Insert name of high-level Kirkland signatory]

Reference Guide

We encourage you to take the following steps:

Register for Identity Monitoring Services.

To help relieve concerns and restore confidence following this incident, we have secured the services of Kroll to provide Minor Identity Monitoring, Fraud Consultation, and Identity Theft Restoration at no cost to you for one year. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data.

Visit **<<IDMonitoringURL>>** to activate and take advantage of your Minor Identity Monitoring services.

You have until <<b2b_text_6 (activation date)>> to activate your Minor Identity Monitoring services.

Membership Number: **<<Membership Number s_n>>**

For more information about Kroll and your Identity Monitoring services, you can visit info.krollmonitoring.com.

KROLL

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You have been provided with access to the following services from Kroll:

Minor Identity Monitoring

Minor Identity Monitoring detects when names, addresses, and credit information is associated with your child's Social Security number. An alert will be sent to you when activity is detected. The presence of a credit file may be an indicator of identity theft or fraud for children who, as minors, should not have a credit history.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge.

To activate services, a U.S. Social Security number and U.S. residential address is required.

Determine Whether Your Student has a Credit File. To determine whether your student has a credit file and, if so, order a free credit report, you may contact each of the three consumer reporting agencies at the contact information listed below.

Equifax, PO Box 740241, Atlanta, GA 30374, www.equifax.com/personal/help/request-child-credit-report/, 1-800-525-6285

Experian, PO Box 9554, Allen, TX 75013, https://www.experian.com/help/minor-request.html, 1-888-397-3742

TransUnion, PO Box 2000, Chester, PA 19016, www.transunion.com/credit-disputes/child-identity-theft-inquiry-form, 1-800-680-7289

Each agency has a different process for checking whether a child has a credit report. Generally, requests on behalf of students under age 13 may be made by mailing the request to each consumer reporting agency. Students age 13 or older may order a free copy of their own credit report by visiting www.annualcreditreport.com or calling toll-free at 1-877-322-8228. Please note that your student may not have a credit report unless you have taken steps to help your student develop a credit history, such as adding them to a credit card in your name. Reports begin when a person applies for and receives credit products, such as loans and credit cards.

If your student has a credit report, review it carefully. Look for accounts you did not open. Look in the "inquiries" section for names of creditors from whom you have not requested credit. Some companies bill under names other than

their store or commercial names. The consumer reporting agency will be able to tell you when that is the case. Look in the "personal information" section for any inaccuracies in your student's information (such as home address and Social Security number). If you see anything you do not understand, call the consumer reporting agency at the telephone number on the report. Errors in this information may be a warning sign of possible identity theft. You should notify the consumer reporting agencies of any inaccuracies in your student's report, whether due to error or fraud, as soon as possible so the information can be investigated and, if found to be in error, corrected. If there are accounts or charges you or your student did not authorize, immediately notify the appropriate consumer reporting agency by telephone and in writing. Consumer reporting agency staff will review your student's report with you. If the information cannot be explained, then you will need to call the creditors involved. Information that cannot be explained also should be reported to your local police or sheriff's office because it may signal criminal activity.

For more information on determining whether your student has a credit file, we encourage you to visit www.annualcreditreport.com/requestingReportsInSpecialSituations.action and the U.S. Federal Trade Commission's ("FTC") website at www.consumer.ftc.gov/articles/0040-child-identity-theft.

Report Incidents. If you detect any unauthorized transactions in a financial account associated with your student, promptly notify the relevant financial institution or payment card company. If you detect any incident of identity theft or fraud, promptly report the incident to law enforcement, the FTC and your state Attorney General. If you believe your student's identity has been stolen, the FTC recommends that you take these steps:

- Close the accounts that you have confirmed or believe have been tampered with or opened fraudulently. For streamlined checklists and sample letters to help guide you through the recovery process, please visit https://www.identitytheft.gov/.
- File a local police report. Obtain a copy of the police report and submit it to relevant creditors and any others that may require proof of the identity theft crime.

You can contact the FTC to learn more about how to protect your student from becoming a victim of identity theft and how to repair identity theft:

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20580
1-877-IDTHEFT (438-4338)

In addition, you can obtain information from the U.S. Department of Education's website about how to protect your student from identity theft: https://studentprivacy.ed.gov/

Consider Placing a Fraud Alert on Your Student's Credit File. To protect your student from possible identity theft, consider placing a fraud alert on your student's credit file. A fraud alert helps protect against the possibility of an identity thief opening new credit accounts in your student's name. When a merchant checks the credit history of someone applying for credit, the merchant gets a notice that the applicant may be the victim of identity theft. The alert notifies the merchant to take steps to verify the identity of the applicant. You can place a fraud alert on your student's credit file in the same manner as described in the "Determine Whether Your Student has a Credit File" section above.

Consider Placing a Security Freeze on Your Student's Credit File. You may wish to place a "security freeze" (also known as a "credit freeze") on your student's credit file. A security freeze is designed to prevent potential creditors from accessing your student's credit file at the consumer reporting agencies without your consent. *Unlike a fraud alert, you must place a security freeze on your student's credit file at each consumer reporting agency individually*. There is no charge to place or lift a security freeze. In some states, even if your student does not have a credit file, you can place a freeze that will make it difficult for someone to use your student's information to open new accounts. For more information on security freezes, you may contact the three nationwide consumer reporting agencies or the FTC as described above. As the instructions for establishing a security freeze differ from state to state, please contact the three nationwide consumer reporting agencies to find out more information.

The consumer reporting agencies may require proper identification prior to honoring your request. For example, in addition to your student's full name, Social Security number, date of birth, and address, you may be asked to provide:

- Your full name with middle initial and generation (such as Jr., Sr., II, III)
- Your Social Security number
- Your date of birth

- Addresses where you have lived over the past five years
- A legible copy of a government-issued identification card (such as a state driver's license or military ID card)
- Proof of your current residential address (such as a current utility bill or account statement)

For New York Residents. You can obtain information from the New York State Office of the Attorney General about how to protect your student from identity theft and tips on how to protect your student's privacy online. You can contact the New York State Office of the Attorney General at:

Office of the Attorney General
The Capitol
Albany, NY 12224-0341
(800) 771-7755
(800) 788-9898
https://ag.ny.gov/

Bureau of Internet and Technology (BIT)
28 Liberty Street
New York, NY 10005
Phone: (212) 416-8433
https://ag.ny.gov/about/about-office/economic-justice-division#internet-technology