

NEW YORK
LONDON
SINGAPORE
PHILADELPHIA
CHICAGO
WASHINGTON, DC
SAN FRANCISCO
SILICON VALLEY
SAN DIEGO
LOS ANGELES
TAIWAN
BOSTON
HOUSTON
AUSTIN
HANOI
HO CHI MINH CITY

Duane Morris®

FIRM and AFFILIATE OFFICES

DIRECT DIAL: +1 619 744 2219
PERSONAL FAX: +1 619 923 2967
E-MAIL: MHDonovan@duanemorris.com

www.duanemorris.com

SHANGHAI
ATLANTA
BALTIMORE
WILMINGTON
MIAMI
BOCA RATON
PITTSBURGH
NEWARK
LAS VEGAS
CHERRY HILL
LAKE TAHOE
MYANMAR
OMAN
A GCC REPRESENTATIVE OFFICE
OF DUANE MORRIS
ALLIANCES IN MEXICO
AND SRI LANKA

April 19, 2019

SUBMITTED VIA ONLINE PORTAL

Attorney General Xavier Becerra
Office of the Attorney General
California Department of Justice

Re: Data Security Incident Notification

Dear Attorney General Becerra:

We are writing on behalf of Mikhail Education Corporation to report a data security incident that occurred March 20 and 26, 2019. During the incident, two email accounts were compromised for a short period of time. While we have no evidence of actual or attempted misuse of personal information, our investigation revealed some personal information was included in these email accounts. We took measures to secure the email accounts immediately after we learned of the incident. We are also reviewing our policies, procedures, and security systems to determine what changes are appropriate to protect personal information stored on our system.

We are uncertain whether any personal information was actually viewed by others. However, we are reaching out to all data subjects potentially affected by this incident and providing them with a complimentary, two-year membership to Experian's IdentityWorks. IdentityWorks includes credit monitoring, identity theft insurance, and identity restoration services.

Up to 1,348 California residents may have been affected by this incident. To provide notification as expeditiously as possible, an initial Notice of Data Breach was sent via email on Friday April 12, 2019 to those individuals for whom email information was available at that time. A final Notice of Data Breach with activation codes for the IdentityWorks subscription will be mailed to all data subjects potentially affected by the breach on or before Monday

Attorney General Xavier Becerra
April 19, 2019
Page 2

April 22, 2019. A sample copy of the notification letter is included with this letter. Notice is also being provided to the credit reporting agencies.

Please contact me if you have any questions or need any additional information regarding this incident.

Very truly yours,

A handwritten signature in blue ink, appearing to read "MHon", with a long horizontal flourish extending to the right.

Michelle Hon Donovan



VIA U.S. MAIL

April XX, 2019

[NAME]
[ADDRESS]
[CITY], [STATE] [ZIP]

RE: Notice of Data Breach

Dear [NAME]:

We are writing to tell you about a data breach at Mikhail Education Corporation, which may have resulted in the disclosure of your personal information. Mikhail operates Advance Training Institute (ATI), Institute for Business & Technology (IBT), Lamson Institute, and National Career Education. During the breach, two email accounts were compromised for a short period of time. While we have no evidence of actual or attempted misuse of personal information, our investigation revealed some personal information was included in these email accounts. We continue to investigate the breach and take steps to mitigate any harm and prevent further disclosures.

While we are uncertain whether your personal information was actually viewed by others, we are reaching out to all students potentially affected by this incident and providing them with a complimentary, two-year membership to Experian's IdentityWorks. IdentityWorks is a credit monitoring and identity theft protection service, which includes identity theft insurance.

Details regarding the incident, information on how to enroll in IdentityWorks, and preventive steps you can take to reduce the chances of identity theft or fraud can be found in the attached Notice of Data Breach.

We know this is an inconvenience and we apologize for any trouble or concern this has caused you. We take the confidentiality of our students and graduates very seriously.

If you have questions about this incident and its implications, you may contact Paul Sapio, Vice President of IT via email at psapio@mikhailed.com or by phone 702.852.1299.

Sincerely,

A handwritten signature in black ink, appearing to read 'Peter Mikhail', with a long horizontal stroke extending to the right.

Peter Mikhail
Chief Executive Officer

Enclosure

Mikhail Education Corporation

April XX, 2019

Notice of Data Breach

What Happened?	During the time period of March 20 th through 26 th , two company email accounts were compromised by a malicious third-party actor. In each instance, the breach incident was detected quickly. Based on our investigation, we believe that the first account was secured within approximately 42 minutes of the initial breach and the second account was secured within approximately 16 minutes of the initial breach. While we have no evidence of actual or attempted misuse of personal information, our investigation revealed some personal information was included in these email accounts.
What Information Was Involved?	One or more of the following categories of personally identifiable information may have been accessed: name, social security number, driver's license number, passport, educational records, and/or medical information, primarily relating to students in select programs that require medical testing. Only the name of the test was potentially accessed, not the results of the tests. The affected information is different for each data subject. Please contact us if you would like to know more about what data was involved.
What Are We Doing?	<p>We took measures to secure the email accounts immediately after we learned of the incident. We are continuing to work to confirm all facts associated with this incident. We are also reviewing our policies, procedures, and security systems to determine what changes are appropriate to protect personal information stored on our system. We are also contacting all students affected by this incident to notify them of the potential disclosure and offering access to a complimentary two-year membership to Experian's IdentityWorks, at no cost. Please note that you have until July 31, 2019 to activate this membership, which will then continue for 24 full months.</p> <p>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. 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). 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.</p> <p>While <u>Identity Restoration assistance is immediately available to you upon enrollment</u>, we also encourage you to activate the fraud detection tools available through Experian IdentityWorks SM as a complimentary one-year membership. This product provides you with superior identity detection and resolution of identity theft. To start monitoring your personal information please follow the steps below:</p> <ul style="list-style-type: none">• Ensure that you enroll by: July 31, 2019 (Your code will not work after this date.)• Visit the Experian IdentityWorks website to enroll: https://www.experianidworks.com/3bcredit• Provide your activation code: [CODE TO BE PROVIDED] <p>If you have questions about the product, need assistance with identity restoration that arose as a result of this incident, or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 877-890-9332 by July 31, 2019 prepared to provide engagement number DB12032 as proof of eligibility for the identity restoration services by Experian.</p> <p>ADDITIONAL DETAILS REGARDING YOUR 24-MONTH EXPERIAN IDENTITYWORKS MEMBERSHIP:</p> <p>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:</p> <ul style="list-style-type: none">▪ 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, Equifax and Transunion files for indicators of fraud.▪ Identity Restoration: Identity Restoration specialists 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.▪ \$1 Million Identity Theft Insurance**: Provides coverage for certain costs and unauthorized electronic fund transfers.

	<p>What you can do to protect your information: There are additional actions you can consider taking to reduce the chances of identity theft or fraud on your account(s). Please refer to www.ExperianIDWorks.com/restoration for this information.</p> <p>* Offline members will be eligible to call for additional reports quarterly after enrolling ** Identity theft insurance is underwritten by insurance company subsidiaries or affiliates of American International Group, Inc. (AIG). 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</p>			
<p>What You Can Do.</p>	<p>While there is no need to take any action unless you become aware of suspicious activity regarding your personal information, there are some preventive steps you can take to reduce the chances of identity theft or fraud on your account(s). This includes activating your complementary 24-month Experian IdentityWorks account and utilizing the fraud detection tools made available to you through this account. If appropriate, you may also want to take one or more the following preventative steps:</p> <p>> <i>Place A 90-Day Fraud Alert On Your Credit File.</i> An initial 90-day security alert indicates to anyone requesting your credit file that you suspect you are a victim of fraud. When you or someone else attempts to open a credit account in your name, increase the credit limit on an existing account, or obtain a new card on an existing account, the lender should take steps to verify that you have authorized the request. If the creditor cannot verify this, the request should not be satisfied. You may contact one of the credit reporting companies below for assistance.</p> <table border="0" data-bbox="389 724 1230 814"> <tr> <td style="text-align: center;">Equifax 1-800-349-9960 www.equifax.com</td> <td style="text-align: center;">Experian 1-888-397-3742 www.experian.com</td> <td style="text-align: center;">TransUnion 1-800- 909-8872 www.transunion.com</td> </tr> </table> <p>> <i>Place A Security Freeze On Your Credit File.</i> If you are very concerned about becoming a victim of fraud or identity theft, a security freeze might be right for you. Placing a freeze on your credit report will prevent lenders and others from accessing your credit report entirely, which will prevent them from extending credit. <i>This means you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze.</i> Security freezes are not shared among the national credit reporting companies. You must request a freeze separately with each of them.</p> <p>> <i>Order Your Free Annual Credit Reports.</i> Visit www.annualcreditreport.com. You are entitled under federal law to one free comprehensive disclosure of all of the information in your credit file from each of the three national credit bureaus every 12 months. 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.</p> <p>> <i>Use Tools From Credit Providers.</i> Carefully review your credit reports and bank, credit card and other account statements. Be proactive and create alerts on credit cards and bank accounts to notify you of activity. If you discover unauthorized or suspicious activity on your credit report or by any other means, file an identity theft report with your local police and contact a credit reporting company.</p> <p>> <i>Rights Under the Fair Credit Reporting Act (FCRA).</i> You may have additional rights under the FCRA. See https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf for a summary.</p>	Equifax 1-800-349-9960 www.equifax.com	Experian 1-888-397-3742 www.experian.com	TransUnion 1-800- 909-8872 www.transunion.com
Equifax 1-800-349-9960 www.equifax.com	Experian 1-888-397-3742 www.experian.com	TransUnion 1-800- 909-8872 www.transunion.com		
<p>For More Information.</p>	<p>To learn more about how to protect yourself after receiving notice of a breach or to report identity theft you can contact the Federal Trade Commission (“FTC”) at: 1-877-ID-THEFT (877-438-4338) or https://www.identitytheft.gov. The general contact information for the FTC is: Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580; (202) 326-2222.</p> <p>For residents of Maryland, North Carolina and Oregon: You can obtain also information about steps you can take to avoid identity theft from your state Attorney General:</p> <table border="1" data-bbox="332 1675 1490 1858"> <tr> <td style="text-align: center;"> <p>Maryland Attorney General Consumer Protection Division 200 St. Paul Place Baltimore MD 21202 1-888-743-0023 www.oag.state.md.us</p> </td> <td style="text-align: center;"> <p>NC Attorney General Consumer Protection Division 9001 Mail Service Center Raleigh, NC 27699-9001 1-877-566-7226; www.ncdoj.com</p> </td> <td style="text-align: center;"> <p>Oregon Attorney General Consumer Protection Division 1162 Court St. NE Salem, OR 97301-4096 1-877-877-9392 www.doj.state.or.us</p> </td> </tr> </table> <p>If you have questions about this incident and its implications, you may contact Paul Sapio, Vice President of IT via email at psapio@mikhailed.com or by phone 702.852.1299.</p>	<p>Maryland Attorney General Consumer Protection Division 200 St. Paul Place Baltimore MD 21202 1-888-743-0023 www.oag.state.md.us</p>	<p>NC Attorney General Consumer Protection Division 9001 Mail Service Center Raleigh, NC 27699-9001 1-877-566-7226; www.ncdoj.com</p>	<p>Oregon Attorney General Consumer Protection Division 1162 Court St. NE Salem, OR 97301-4096 1-877-877-9392 www.doj.state.or.us</p>
<p>Maryland Attorney General Consumer Protection Division 200 St. Paul Place Baltimore MD 21202 1-888-743-0023 www.oag.state.md.us</p>	<p>NC Attorney General Consumer Protection Division 9001 Mail Service Center Raleigh, NC 27699-9001 1-877-566-7226; www.ncdoj.com</p>	<p>Oregon Attorney General Consumer Protection Division 1162 Court St. NE Salem, OR 97301-4096 1-877-877-9392 www.doj.state.or.us</p>		