

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

MICHELLE HON DONOVAN
DIRECT DIAL: 619 744 2219
PERSONAL FAX: 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

RECEIVED
FEB 06 2018
CONSUMER PROTECTION

February 5, 2018

VIA FEDEX

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

RE: DATABASE BREACH NOTIFICATION

Dear Attorney General MacDonald:

We are writing on behalf of our client Make-up Designory to report a data breach that occurred as a result of a mailing error made by our client's service provider when it mailed 1098-T Tuition Statements to its students and graduates.

Each January Make-up Designory is required to send a tax document (1098-T Tuition Statement) to its students and graduates, which includes the following information: first and last name, mailing address, social security number, total amount billed for qualified tuition and related expenses and any scholarships or grant totals for the applicable tax year. This information is gathered by its accounting office and then securely transferred to a certified public accounting firm. The accounting firm works with a financial communications service provider that specializes in creating and mailing these and similar type tax forms to be sent by US mail.

This year was no different, except an error occurred in the preparation of the mailings that caused three individual tax documents to be placed in one envelope. As a result, some students received their own 1098-T Tuition Statements and Statements for two other students. This error was not caused by a breach to any computer systems of Make-up Designory or its service providers. The error was caused by human error when our vendor's employee failed to separate the 8.5x11 printed sheet into 1/3 individual 1098-T forms.

DUANE MORRIS LLP

750 B STREET, SUITE 2900 SAN DIEGO, CA 92101-4681

PHONE: +1 619 744 2200 FAX: +1 619 744 2201

Gordon MacDonald
Office of the Attorney General
February 5, 2018
Page 2

The Statements were mailed on January 24, 2018. The vendor notified our client of their error on January 25, 2018. Four (4) New Hampshire residents were potentially affected by this error. However, we believe that the actual number to be lower as one-third of the students in this mailing actually received their own Statements, which means their information was not actually disclosed.

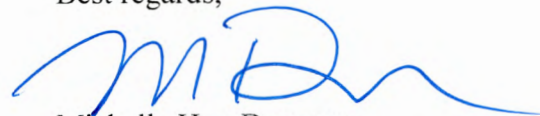
We are contacting all students affected by this incident to notify them of the unintentional disclosure and requesting the return of all 1098-T Statements that were mailed in error. We will follow-up with all such students to confirm that the Statements are returned to the school and/or destroyed.

Make-up Designory sent the attached Notice of Data Breach to all potentially affected consumers on February 3, 2018. It will also be providing a complementary one-year membership to Experian's IdentityWorks, regardless of whether their personal information was actually disclosed. IdentityWorks is a credit monitoring and identity theft protection service, which includes identity theft insurance.

Our client's third party mailing service provider was carefully vetted prior to use. They have been mailing confidential tax documents for over 30 years and have never before had an incident. We are in the processes of reviewing the vendor's security policies and procedures to ensure that a similar mistake is not repeated.

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

Best regards,



Michelle Hon Donovan

MHD:ms
Enclosure

SCHOOL LETTERHEAD
Address

NOTICE OF DATA BREACH

February 3, 2018
[Insert Name]
[Address]
[City, State Zip]

VIA E-MAIL AND U.S. MAIL

Dear [Name]:

We are writing to let you know that a mailing error occurred when our service provider mailed your 1098-T Tuition Statement, which may have resulted in the disclosure of your personal information. 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 an identity theft protection plan and identity theft insurance.

Each January we are required to send a tax document (1098-T Tuition Statement) to students and graduates that states the amount of money given to the school the previous year for tuition. The information is gathered by our accounting office and then securely transferred to a certified public accounting firm. The accounting firm works with a financial communications service provider that specializes in creating these and similar type tax forms to be sent by US mail. This year was no different, except an error occurred in the preparation of the mailings that caused three individual tax documents to be placed in one envelope. As a result, some students received their own 1098-T Tuition Statements and Statements for two other students. This error was not caused by a breach to any computer systems of MUD or its service providers. The error was caused by human error when our vendor's employee failed to separate the 8.5x11 printed sheet into 1/3 individual 1098-T forms.

Our third party mailing service provider was carefully vetted prior to use. They have been mailing confidential tax documents for over 30 years and have never before had an incident. We are in the processes of reviewing the vendor's security policies and procedures to ensure that a similar mistake is not repeated.

If you received an envelope with three Statements, then your personal information has remained confidential and you are not affected by this incident. However, we would like your assistance to ensure other students' information is protected.

- If you received a 1098-T Tuition Statement from MUD postmarked January 24, 2018 and have not opened it – do not open the envelope. Please help us keep this information confidential by returning the envelope unopened to in person or by mail to the MUD Campus you attended. A replacement 1098-T Tuition Statement has already been mailed to you.

- If you received a 1098-T Tuition Statement from MUD and have already opened it – please return the Tuition Statements that do not belong you to the MUD Campus you attended, either in person or by mail.
- If you received a 1098-T Tuition Statement from MUD and already threw away or destroyed the Tuition Statements that do not belong you, please contact Christy Ruoff, at christy@mud.edu or 818-729-9420 to let us know.

We will be following up with all students who received an incorrect Statements to confirm that all such Statements have been returned to the school and/or destroyed.

MUD will also be offering you and all affected students a complimentary, one-year membership to Experian's IdentityWorks regardless of whether your personal information was disclosed. 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 on your account 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. It is for this reason, that we have used a third party that specializes in the distribution of confidential information. Unfortunately, our best intentions aside, a human error occurred.

If you have questions about this incident and its implications, you may contact Christy Ruoff, Director of Financial Aid, at christy@mud.edu or by phone at 818-729-9420.

Thank you for your help and understanding.

Sincerely,

Tate Holland
President

Enclosure

Make-up Designory
February 3, 2018

Notice of Data Breach

<p>What Happened?</p>	<p>A mailing error caused Students' 1098-T Tuition Statements to be included in another student's mailing envelope, and the Statements were inadvertently mailed to another student on January 24, 2018.</p>
<p>What Information Was Involved?</p>	<p>1098-T Tuition Statements contain your first and last name, mailing address, social security number, total amount billed for qualified tuition and related expenses for 2017 and any scholarships or grant totals for 2017.</p>
<p>What Are We Doing?</p>	<p>We are contacting all students affected by this incident to notify them of the unintentional disclosure and requesting the return of all 1098-T Statements that were mailed in error. We will follow-up with all such students to confirm that the Statements are returned to the school and/or destroyed.</p> <p>We are also offering you access to a complimentary one-year membership to Experian's IdentityWorks, at no cost to you. Please note that you have until May 31, 2018 to activate this membership, which will then continue for 12 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).</p> <p>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 IdentityWorksSM 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: March 31, 2018 (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] <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</p>

by March 31, 2018 prepared to provide engagement number **DB05224** as proof of eligibility for the identity restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 12-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, 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.

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.

* 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

What You Can Do.

While there is no need not 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 12 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:

➤ **Place A 90-Day Fraud Alert On Your Credit File**

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.

Equifax
1-800-349-9960
www.equifax.com

Experian
1-888-397-3742
www.experian.com

TransUnion
1-800- 909-8872
www.transunion.com

➤ **Place A Security Freeze On Your Credit File**

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. *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.* Security freezes are not shared among the national credit reporting companies. You must request a freeze separately with each of them. Credit reporting companies may charge a fee to freeze and unfreeze your account.

➤ **Order Your Free Annual Credit Reports**

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 once 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.

➤ **Manage Your Personal Information**

Take steps such as: carrying only essential documents with you; being aware of whom you are sharing your personal information with and shredding receipts, statements, and other sensitive information.

➤ **Use Tools From Credit Providers**

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.

For More Information.

To learn more about how to protect yourself after receiving notice of a breach or to report identity theft to the Federal Trade Commission ("FTC"), you can go to the FTC's Web site at www.ftc.gov/idtheft. You can file an identity theft complaint with the FTC by using the FTC's Identity Theft Hotline at: 1-877-ID-THEFT (877-438-4338) or online at <https://www.identitytheft.gov>. The general contact information for the FTC is listed below:

Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580
(202) 326-2222

If you have questions about this incident and its implications, you may contact Christy Ruoff, Director of Financial Aid at christy@mud.edu or by phone at 818-729-9420.