

MARIO AYOUB
mayoub@bsk.com
P: 716.416.7023
F: 716.416.7001

January 13, 2025

VIA ELECTRONIC MAIL (IDTHEFT@OAG.STATE.MD.US)

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202

Re: *Notice of Data Incident*

To Whom It May Concern:

We represent Relay Graduate School with respect to a recent data incident. On November 22, 2024, Relay discovered that a threat actor gained access to several Relay applications hosted by Amazon Web Services ("AWS") and deleted certain files stored on the AWS environment. Despite taking prompt remedial action, which included severing the threat actor's access to the environment, the threat actor may have been able to access certain student records containing personally identifiable information. On December 11, 2024, after successfully restoring the deleted files from backups and confirming the population of potentially impacted individuals, Relay learned personal information associated with 487 Maryland residents may have been impacted. Due to the immediate response time of the AWS security team and Relay's cybersecurity team, the unauthorized access was limited to a few hours.

The following data elements potentially involved include: (1) full names; (2) contact information, such as mailing addresses, email addresses, and phone numbers; and (3) dates of birth. While Social Security numbers are stored in the environment, they are encrypted. There is no evidence to indicate that the threat actor was able to circumvent Relay's security measures and access any Social Security numbers. However, out of an abundance of caution, Relay is providing all potentially impacted individuals with free credit monitoring services. To date, Relay has not discovered any instance of identity theft or fraud associated with this incident.

As soon as Relay learned of this incident, Relay took affirmative steps to sever the threat actor's access, reset IT passwords, and harden its network. Relay also engaged cybersecurity counsel and a forensics firm to guide it through the incident response process, confirm that the threat actor was no longer in Relay's system, and further harden its network against future attacks. Relay has reported this incident to federal law enforcement and will cooperate with any subsequent investigation.

Maryland Office of the Attorney General
January 13, 2025
Page 2

The attached notification template was mailed to Maryland residents on January 10, 2025. Relay apologizes for any inconvenience this incident may have caused and remains steadfast in its commitment to protect personal information.

Very truly yours,

BOND, SCHOENECK & KING, PLLC

A handwritten signature in dark ink, appearing to read "Mario Ayoub", written over a light gray rectangular background.

Mario Ayoub

(Attachment)

Relay Graduate School of Education
c/o Cyberscout
<Return Address>
<City>, <State> <Zip>



<<FirstName>> <<LastName>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<PostalCode+4>>

January 10, 2025

Notice of Breach

Dear <<FirstName>> <<LastName>>:

We are writing to inform you of a recent security incident at Relay Graduate School of Education that may have impacted your personal information. We take the protection of your personal information very seriously and want to provide you with details, explain the services we are making available to you, and let you know that we continue to take significant measures to protect your information.

What Happened?

On November 22, 2024, we discovered that a threat actor gained access to several Relay applications hosted by Amazon Web Services ("AWS") and deleted certain files stored on the AWS environment. Despite taking prompt remedial action, which included severing the threat actor's access to the environment, the threat actor may have been able to access certain student records containing personally identifiable information. On December 11, 2024, after successfully restoring the deleted files from backups and confirming the population of potentially impacted individuals, we learned that your personal information may have been impacted. Due to the immediate response time of the AWS security team and our cybersecurity team, the unauthorized access was limited to a few hours.

What Information Was Involved?

The following data elements potentially involved include: (1) your full name; (2) contact information, such as your mailing address, email address, and phone number; and (3) date of birth. While Social Security numbers are stored in the environment, they are encrypted. There is no evidence to indicate that the threat actor was able to circumvent Relay's security measures and access any Social Security numbers. However, out of an abundance of caution, we are providing you with free Credit Monitoring services as described below. To date, we have not discovered any instance of identity theft or fraud associated with this incident.

What We Are Doing

As soon as we learned of this incident, we took affirmative steps to sever the threat actor's access, reset IT passwords, and harden our network. We also engaged cybersecurity counsel and a forensics firm to guide us through the incident response process, confirm that the threat actor was no longer in our system, and further harden our network against future attacks. We have reported this incident to federal law enforcement and will cooperate with any subsequent investigation.

In response to the incident, we are providing you with 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 <<service length>> from the date of enrollment when changes occur to your credit file. This notification is sent to you the same day that the change or update takes place with the bureau. Finally, we are providing you with proactive fraud assistance to help with any questions 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 You Can Do

Although there is no indication that Social Security numbers were impacted, we encourage you to take advantage of our free Credit Monitoring services. To enroll in Credit Monitoring services at no charge, please log on to <https://bfs.cyberscout.com/activate> and follow the instructions provided. When prompted please provide the following unique code to receive services: <<UniqueCode>>. In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter. The enrollment requires an internet connection and e-mail account and may not be available to minors under the age of 18 years of age. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

In addition, please refer to the enclosed Recommended Steps document to learn more about additional actions you can take to protect your information.

For More Information

If you have questions regarding this incident, please contact us through our dedicated call center. Representatives are available for 90 days from the date of this letter, to assist you with questions regarding this incident, between the hours of 8:00 a.m. to 8:00 p.m. Eastern time, Monday through Friday, excluding holidays. Please call the help line at 1-833-799-4261 and supply the representative with your unique code listed above.

We apologize for any inconvenience this incident may have caused.

Sincerely,

A handwritten signature in dark ink, appearing to read 'M. Hostetter', with a stylized, cursive-like script.

Dr. Mayme Hostetter

President – Relay Graduate School of Education.

Recommended Steps to help Protect your Information

1. Review your credit reports. We recommend that you remain vigilant by reviewing account statements and monitoring credit reports. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

You should also know that you have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to the Attorney General. You have the right to obtain a police report.

2. Place Fraud Alerts with the three credit bureaus. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. You can place a fraud alert at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. The contact information for all three bureaus is as follows:

Credit Bureaus

Equifax Fraud Reporting
1-866-349-5191
P.O. Box 105069
Atlanta, GA 30348-5069
www.equifax.com

Experian Fraud Reporting
1-888-397-3742
P.O. Box 9554
Allen, TX 75013
www.experian.com

TransUnion Fraud Reporting
1-800-680-7289
P.O. Box 2000
Chester, PA 19022-2000
www.transunion.com

It is necessary to contact only ONE of these bureaus and use only ONE of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well. You will receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review. An initial fraud alert will last for one year.

Please Note: No one is allowed to place a fraud alert on your credit report except you.

3. Security Freeze. By placing a security freeze, someone who fraudulently acquires your personal identifying information will not be able to use that information to open new accounts or borrow money in your name. You will need to contact the three national credit reporting bureaus listed above to place the freeze. Keep in mind that when you place the freeze, 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. There is no cost to freeze or unfreeze your credit files.

4. You can obtain additional information about the steps you can take to avoid identity theft from the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

California Residents: Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft. Office of the Attorney General of California, 1300 I Street, Sacramento, CA 95814, Telephone: 1-800-952-5225.

Kentucky Residents: Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601, www.ag.ky.gov, Telephone: 1-502-696-5300.

Maryland Residents: Office of the Attorney General of Maryland, Consumer Protection Division 200 St. Paul Place Baltimore, MD 21202, www.oag.state.md.us/Consumer, Telephone: 1-888-743-0023.

New Mexico Residents: You have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit “prescreened” offers of credit and insurance you get based on information in your credit report; and you may seek damages from a violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. You can review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

New York Residents: the Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; <https://ag.ny.gov/>.

North Carolina Residents: Office of the Attorney General of North Carolina, 9001 Mail Service Center Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 1-919-716-6400.

Oregon Residents: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 1-877-877-9392

Rhode Island Residents: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 1-401-274-4400

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, <https://consumer.ftc.gov>, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.