From: "Lisa Avila; William Mynster" <email@totalregistration.net>
Date: May 30, 2019 at 1:09:50 PM PDT
To: "Lan Yang"
Subject: Notice of Data Security Incident
Reply-To: lavila@fjuhsd.org; wmynster@fjuhsd.org

Dear Lan,

The privacy and protection of students' information is a matter we take very seriously, which is why, as a precautionary measure, we are writing to let you know about a data security incident with one of our third-party service providers that may have involved your personal information. Below is a summary of the incident, and Total has also created a Frequently Asked Questions (FAQ) webpage summarizing the details of the incident, available at https://TotalRegistration.net/DSI-FAQ.php

WHAT HAPPENED?

Total Registration LLC ("Total Registration") facilitates exam registration for Troy High School students, including Advanced Placement, International Baccalaureate, and PSAT/NMSQT examinations. On May 10, 2019, Total Registration informed us that it had received notice of a misconfigured server that allowed for the potential unauthorized access to some of the information that Total Registration stores on its systems. Total Registration was informed of this issue on the evening of April 11, 2019, by a security researcher and reporter who wanted to make sure that Total Registration's information was not improperly accessed or misused.

Upon receipt of this information, Total Registration immediately investigated and remedied the issue by April 12, 2019. As part of that investigation, Total Registration discovered that one of its developers misconfigured a setting within its Amazon S3 file storage service. Total Registration uses this S3 file storage service to store reports and registration confirmations created by its users. As a result of that configuration, certain files (pdf, .csv, .doc) that individual schools can create from reports, which list information about students registered for exams, and copies of registration confirmations generated by individual registrants, may have been available to individuals with knowledge of S3 system architecture who accessed the URL for the Total Registration S3 file storage.

All school-generated reports or student-generated confirmations were only accessible for 48 hours after the applicable file or confirmation was generated. After 48 hours, each report or confirmation would automatically be deleted. *It is important to note that based upon Total Registration's investigation, only those reports that a user chose to save in .pdf, .csv, or .doc file format were accessible. If a user viewed or printed a report but did not elect to generate or save a .pdf, .csv, .doc file, there was no file stored in S3.* Total Registration set up the S3 file storage service in June 2016, so any files that were created and stored on the S3 service between June 2016 and April 12, 2019, would have been accessible during the 48-hour window between that file's creation date and its automatic deletion by Total Registration.

WHAT INFORMATION WAS INVOLVED?

The data that may have been exposed was limited to certain information used to register for Advanced Placement, International Baccalaureate, and PSAT/NMSQT exams, based on how individual schools conducted registrations and ran their reports. Those reports may have included student registration information that students provided when registering for a test, such as name, (of students and/or parents), date of birth, language, grade level, sex, student ID, last four digits of Social Security Number (of International Baccalaureate registrants only), physical address (of students and/or parents), email addresses (of students and/or parents), phone numbers (of students and/or parents), ethnicity,International Baccalaureate candidate category, and College Board identification number (e.g., SSD), as well as some additional information that may be requested by individual schools for their registrations.

WHAT INFORMATION WAS NOT INVOLVED?

The data that may have been exposed **DID NOT** include:

- Full Social Security Numbers
- Credit Card Numbers, cvv codes or expiration dates
- Medical Information
- Passwords or security questions
- Any test results or scores

WHAT IS TOTAL REGISTRATION DOING?

Total Registration immediately reconfigured its settings for its file storage system to correct the problem. It has also deleted any remaining files in the S3 file storage service that had been retained due to the misconfigured setting. Total Registration is working with a third-party data security specialist to review its platform to make sure that this type of incident does not happen again. It is also implementing additional security measures designed to prevent a recurrence of such an incident.

Total Registration will continue to follow up with us regarding this incident and any further investigations and security measures that it may take.

WHAT CAN YOU DO?

Total Registration has informed us that, except for the individual who notified Total Registration of the misconfigured server, it is not aware of (nor is there any evidence of) any third-party who accessed information that may have been exposed as a result of this incident.

Given the types of information that may have been accessible as part of this incident, we do not believe that there is a risk of identity theft or harm from this incident. However, we encourage you to take usual prudent precautions with your personal data. You should not open emails from any unknown senders. You should never open untrusted web links. You should never provide personal information via email or over the phone to any unverified entity. Total Registration will never contact families to update financial information or provide additional information.

We also encourage you to remain vigilant for occurrences of fraud and identity theft by regularly reviewing your account statements and monitoring free credit reports for any unauthorized activity. If you discover any suspicious or unusual activity on your accounts, be sure to report it immediately to your financial institutions, as major credit card companies have rules that restrict them from requiring you to pay for fraudulent charges that are timely reported.

Due to the nature of the incident and the type of data potentially vulnerable, Total Registration will not be offering identity protection or credit monitoring services.

GENERAL WAYS TO PROTECT YOUR IDENTITY

Families that are concerned about these issues are encouraged to take advantage of the following services:

You may contact the Federal Trade Commission (FTC) or law enforcement, such as your state attorney general, to report incidents of identity theft or to learn about steps you can take to protect yourself from identity theft. You can contact the FTC at:

Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580
(877) IDTHEFT (438-4338)
https://www.identitytheft.gov/

If you find that your information has been misused, the FTC encourages you to file a complaint with the FTC and to take these additional steps: (1) close the accounts that you have confirmed or believe have been tampered with or opened fraudulently; and (2) file and keep a copy of a local police report as evidence of the identity theft crime.

Obtain Your Credit Report

You may periodically obtain a copy of your credit report from each nationwide credit reporting agency. If you discover inaccurate information or a fraudulent transaction on your credit report, you have the right to request that the credit reporting agency delete that information from your credit report file.

In addition, under federal law, you are entitled to one free copy of your credit report every 12 months from each of the three nationwide credit reporting agencies. You may obtain a free copy of your credit report by going to www.AnnualCreditReport.com or by calling (877) 322-8228. You also may complete the Annual Credit Report Request Form available from the FTC at https://www.consumer.ftc.gov/articles/pdf-0093-annual-report-request-form.pdf, and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. You may also contact any of the three major credit reporting agencies to request a copy of your credit report.

Place a Fraud Alert or Security Freeze on Your Credit Report File

In addition, you may obtain information from the FTC and the credit reporting agencies about fraud alerts and security freezes. A fraud alert can make it more difficult for someone to get credit in your name because it tells creditors to follow certain procedures to protect you, but it also may delay your ability to obtain credit. If you suspect you may be a victim of identity theft, you may place a fraud alert in your file by calling just one of the three nationwide credit reporting agencies listed below. As soon as that agency processes your fraud alert, it will notify the other two agencies, which then must also place fraud alerts in your file. An initial fraud alert will last 90 days. An extended alert stays on your file for seven years. To place either of these alerts, a consumer reporting agency will require you to provide appropriate proof of your identity, which may include your Social Security number. If you ask for an extended alert, you will have to provide an identity theft report.

Also, you can contact the nationwide credit reporting agencies regarding if and how you may place a security freeze on your credit report. A security freeze prohibits a credit reporting agency from releasing information from your credit report without your prior written authorization, which makes it more difficult for unauthorized parties to open new accounts in your name. However, please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing, or other services. The credit reporting agencies have 3 business days after receiving a request to place a security freeze on a consumer's credit report. You may be charged to place or lift a security freeze. Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company.

You may contact the nationwide credit reporting agencies at:

Equifax
P.O. Box 105788
Atlanta, GA 30348
www.equifax.com
(800) 525-6285

Experian
P.O. Box 9554
Allen, TX 75013
www.experian.com
(888) 397-3742

TransUnion
P.O. Box 2000
Chester, PA 19016
www.transunion.com
(800) 680-7289

FOR MORE INFORMATION

We apologize for any inconvenience caused by this incident. You can find answers to most questions at Total Registration's Data Security Incidence - Frequently Answered QuestionsTotalRegistration.net/DSI-FAQ.php. If you have any questions regarding this incident or if you desire further information or assistance, please do not hesitate to contact us at 714-626-4413 or 714) 626-4401.

Sincerely,

William V. Mynster, Ph.D., Principal
wmynster@fjuhsd.org

Lisa A. Avila, AP Coordinator/Counselor

lavila@fjuhsd.org